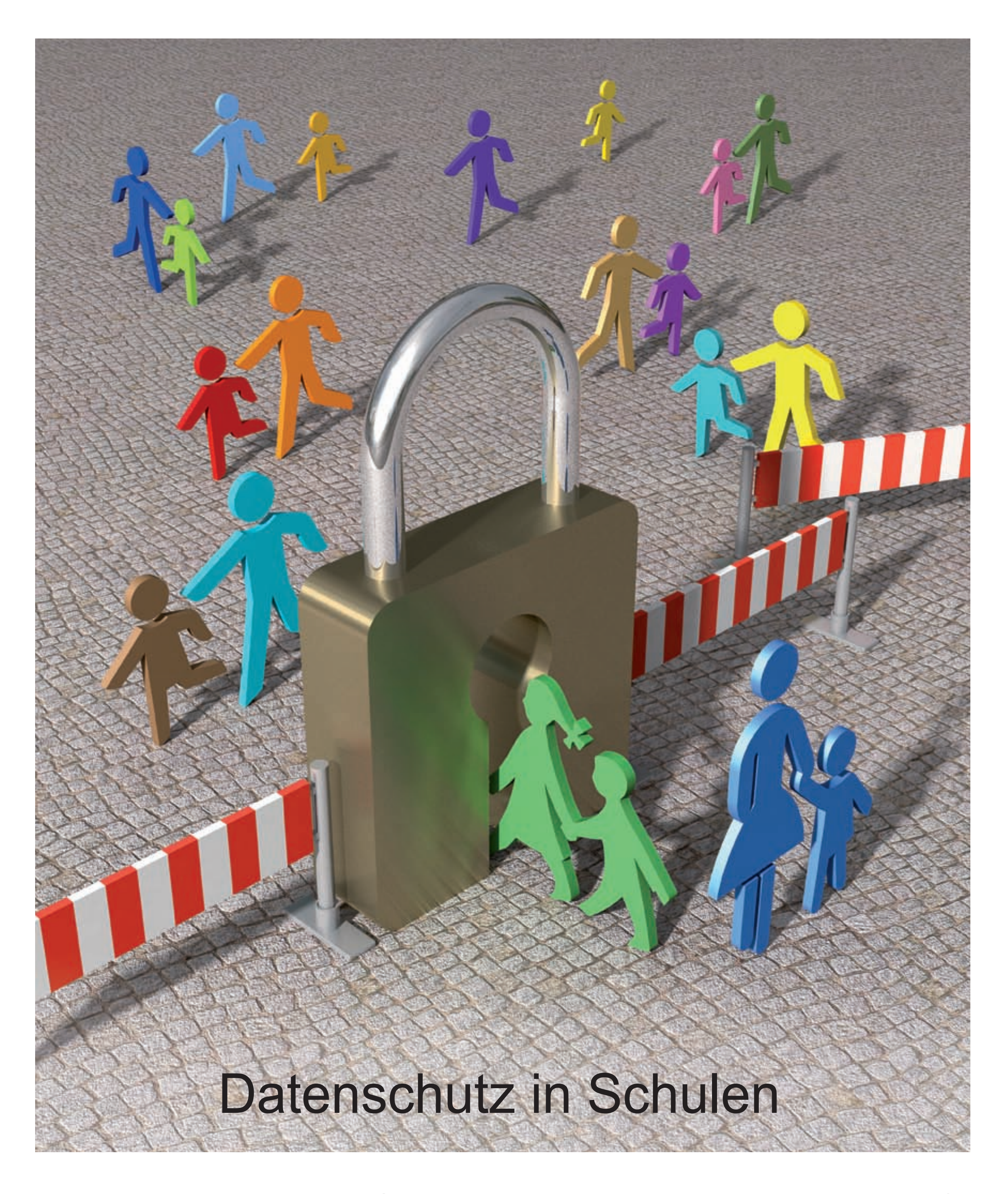
4/2011

Datenschutz Nachrichten

34. Jahrgang
ISSN 0137-7767
9,00 Euro



Datenschutz in Schulen

■ Datenschutzpraxis an Schulen – Nachsitzen ist angesagt ■ Hilfe gibt es bei den Landesdatenschutzbeauftragten ■ Datenschutz in der Schule ■ Schulverwaltungsdaten auf privaten Rechnern der Lehrkräfte ■ Dopingbekämpfung und Persönlichkeitsschutz ■ Presseerklärungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Samstag, 07 Januar 2012
Kamingespräch
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 08 Januar 2012
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Mittwoch, 18. April 2012
Datenschutz in der Medizin: Rechtliche und technische Entwicklungen im Gesundheitsbereich und ihre Relevanz für den Datenschutz
www.update-bdsg.com/html/18-04-2012.html

Montag – Freitag, 13.-17. Februar & 19.-23. März 2012
Weiterbildung für den Betriebsrat zur zertifizierten Fachkraft für Datenschutz bei SAP-Systemen
dtb – Datenschutz-und Technologieberatung Kassel
www.dtb-kassel.de

Freitag, 13 April 2012
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 13. April 2012
Verleihung der BigBrotherAwards 2012
Bielefeld
http://www.bigbrotherawards.de

Dienstag – Donnerstag, 22. – 24. Mai 2012
Compliance oder Mitarbeiterkontrolle? Arbeitsrecht und Datenschutz
dtb – Datenschutz-und Technologieberatung Kassel
www.dtb-kassel.de

Freitag, 9. November 2012
FIfF Jahrestagung 2012
Hochschule Fulda
www.fiff.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
34. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Hajo Köppen
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Frans Jozef Valenta

Nachsitzen

für Lehrkräfte und Schulleitungen in Sachen Datenschutz! Zu diesem Ergebnis führt zumindest die Lektüre der Berichte zum Schuldatenschutz in den Tätigkeitsberichten der Landesdatenschutzbeauftragten. Die Vielzahl der (offensichtlich als „Spitze des Eisberges") geschilderten Sachverhalte über meist gravierende Datenschutzverstöße verwundert umso mehr, da gerade die Schule als zentraler, grundlegender gesellschaftlicher Lernort die Förderung, Vermittlung, Umsetzung und Wahrnehmung der für ein demokratisches Gemeinwesen unverzichtbaren Persönlichkeits- und Datenschutzrechte leisten muss. Nicht zuletzt durch gutes Vorbild bei der Umsetzung der Vorgaben des Datenschutzrechts im Umgang mit persönlichen Informationen über Schüler, Lehrer und Eltern. Wie soll man glaubwürdig den Umgang mit modernen Informations- und Kommunikationstechnologien incl. Datenschutzrecht vermitteln, wenn es um die Praxis in der Schule nicht zum Besten steht? Wie sollen sich zum Beispiel Lehrkräfte glaubwürdig über von Schülern bei Facebook eingestellte Lehrerfotos beklagen, wenn die Schule gleichzeitig ohne Einwilligung der Schüler deren Bilder auf der Schul-Homepage weltweit zum Abruf bereit hält?

Dabei wird konzediert, dass das Datenschutzrecht nicht gerade eine einfache Rechtsmaterie darstellt und teilweise einen komplizierten Paragrafen-Dschungel bietet, in dem man sich durchaus verirren kann. Aber auch die Vermittlung der nicht gerade „leichten" deutschen Grammatik, hochkomplexer mathematischer Sachverhalte, biologischer, physikalischer und chemischer Vorgänge, um nur einige Beispiel zu nennen, wird von der Schule geleistet.

Informationsmaterial zum Datenschutz sowohl für den Unterricht wie zur Umsetzung datenschutzrechtlicher Vorgaben in der Schulverwaltung liegen ausreichend vor. Sie müssen nur abgerufen und in die Praxis umgesetzt werden. Und auch die staatlichen Datenschützer helfen gerne weiter bei der konsequenten Umsetzung des informationellen Selbstbestimmungsrechts im Schulalltag. Dazu will auch dieses Heft der DANA einen Beitrag leisten.

Hajo Köppen

Autorinnen und Autoren dieser Ausgabe:

Dr. Gabriele Heyse
stellvertretende Direktorin des Amtsgerichts Bad Homburg, 2006 bis 2008 im Bundesministerium der Justiz Referentin für Presse- und Öffentlichkeitsarbeit für IT und Datenschutz zuständig.

Hajo Köppen
Assessor. jur., Planungsreferent, Datenschutzbeauftragter und Dozent für Datenschutzrecht an der Technischen Hochschule Mittelhessen;
Kontakt: hajo.koeppen@verw.thm.de.

Karsten Neumann
Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a.D., Stralsund.
neumann@baltic-privacy-management.eu.

Uli Vormwald
Direktor am AfL, seit 1995 im Hessischen Schuldienst, 2006 bis 2009 abgeordnet an das Hessische Kultusministerium mit den Arbeitsschwerpunkten IT-Sicherheit und Datenschutz und in den Jahren 2009 bis 2011 an das Haus des Lebenslangen Lernens in Dreieich, Arbeitsschwerpunkt digitale Medien.

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel,
weichert@datenschutzzentrum.de

Manfred Weitz
Jurist, war bis 2009 Referatsleiter beim Hessischen Datenschutzbeauftragten und dort auch zuständig für den Bereich Datenschutz in Schulen.

Hajo Köppen

Datenschutzpraxis an Schulen – Nachsitzen ist angesagt!

Geht es um den Umgang mit modernen Informations- und Kommunikationstechnologien wie etwa dem Internet, dann leben Lehrer und Schüler häufig in verschiedenen Welten. So das Fazit einer Studie der Landesanstalt für Medien Nordrhein-Westfalen (LfM) über „Medienkompetenz in der Schule“.[1] Während die Nutzung von Online-Netzwerken bei Schülerinnen und Schülern ungemein populär und fester Bestandteil der täglichen Kommunikation ist, sehen, so die Studie, Lehrerinnen und Lehrer die Nutzung von Facebook und andern „sozialen Netzwerken“ eher kritisch. Mit der Folge, dass lediglich 40 % der 1.400 in die Untersuchung einbezogenen Lehrkräfte angaben, ihre Schüler mindestens einmal im Monat mit neuen Medien arbeiten zu lassen. Lediglich 15 % der Lehrkräfte setzen die digitalen Medien mehrmals pro Woche ein, ganz auf ihre Nutzung verzichten immerhin noch 5 %. Blogs und Wikis haben der Umfrage nach 80 % der Befragten noch nicht im Unterricht eingesetzt. Geht man davon aus, dass die Schule die zentrale Lern- und Bildungsinstanz sein soll, die Heranwachsende auf das Leben in der Gesellschaft vorbereitet, also auch auf den Umgang mit modernen Informations- und Kommunikationstechnologien, dann sieht die schulische Praxis nicht sonderlich gut aus. Oder wie es ein Vertreter des Ministeriums für Schule und Weiterbildung des Landes NRW formulierte: „Wir alle, die wir in Schule organisatorisch und pädagogisch Verantwortung tragen, haben die pädagogischen Chancen der Neuen Medien und deren Relevanz für die Lebenswelt der heutigen Schülerinnen und Schüler noch nicht in vollem Umfang erkannt.“[2]

Untrennbar verbunden mit der Vermittlung von Fähigkeiten im Umgang mit den sich rasant entwickelnden Anwendungen der Informations- und Kommunikationstechnologien sind Fragen der Datensicherheit und des Datenschutzes. Wenn aber schon das „Oberthema“ Medienkompetenz wie beschrieben nur eine untergeordnete Rolle in der Unterrichtspraxis spielt, dann dürfte es bei dem „Teilaspekt“ Datenschutz und -sicherheit nicht viel besser bzw. noch schlechter stehen. Und wenn, wie in Niedersachsen, ein Internetportal „Medienkompetenz-Niedersachsen.de“ zur Vernetzung der vorhandenen Internetplattformen zur Medienbildung und Medienerziehung geschaffen wird, dann spielt das Thema Datenschutz nur eine untergeordnete Rolle.[3]

Wirft man einen Blick in die Tätigkeitsberichte[4] der Landesdatenschutzbeauftragten und deren Berichte aus der schulischen Datenschutzpraxis von Lehrerinnen und Lehrern sowie Schulleitungen, so findet man für diese Annahme eine gewisse Bestätigung. „Im Schulbetrieb lauern zahlreiche datenschutzrechtliche Fallstricke. Das Problembewusstsein der Verantwortlichen ist manchmal aber nur schwach ausgeprägt“. So der Kommentar des Landesdatenschutzbeauftragten in Baden-Württemberg zur Situation des Datenschutzes an Schulen.[5] Der Hamburgische Datenschutzbeauftragte formulierte es so: „Die Beispiele zeigen aber, dass die Vermittlung datenschutzrechtlicher Grundsätze bei den Lehrkräften noch verbesserungswürdig ist. Besonders gefordert hierbei sind die Schulleitungen und die Behörde für Schule und Berufsbildung.“[6] Ein Fazit, das auch von anderen Datenschützern gezogen wird und zu einer Reihe von Aktivitäten geführt hat, um Datenschutzbewusstsein und –kenntnisse bei Beschäftigten an Schulen zu fördern. So hat etwa der Schleswig-Holsteinische Datenschutzbeauftragte ein 222 Seiten umfassendes „Praxishandbuch Schuldatenschutz“[7] herausgegeben, in Hessen wurde die Broschüre „Datenschutz in Schulen“ veröffentlicht[8]. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) hat die Initiative „Datenschutz geht zur Schule“ gestartet, die sich die Sensibilisierung von Schülerinnen und Schülern der Sekundarstufen I und II im Umgang mit dem Internet und modernen Kommunikationsmedien zum Ziel gesetzt hat.[9] Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz bietet für Schulen Schülerworkshops zum Thema „Datenverantwortung und Datenschutz“ und eigene Unterrichtsmaterialien an.[10] Und auch die 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder äußerte sich zu dem Thema[11]: „Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter – deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.“ Auch von Kultusministerien werden Internetportale zum Thema Datenschutz angeboten, die auf die schulische Praxis ausgerichtet sind und praxisbezogene Hilfestellungen geben.[12]

Die Vielzahl der Materialien und Aktivitäten zum Datenschutz an Schulen, von denen hier nur einige exemplarisch aufgeführt sind, sind sicher auch Ausdruck des erheblichen Nachholbedarfs in der Datenschutzpraxis von Schulen.

Inhaltskontrolle von Schüler-Mobiltelefonen

Unter der Überschrift „Wenn Lehrer zu Hilfspolizisten werden – Einziehung und Inhaltskontrolle von Schüler-Handys“ beschreibt der Berliner

Datenschutzbeauftragte in seinem Tätigkeitsbericht für das Jahr 2006 folgenden Sachverhalt: „Die Mutter eines Schülers beschwerte sich bei uns darüber, dass Lehrkräfte an der Schule ihres Sohnes die Handys einer ganzen Klasse eingezogen und deren gespeicherte Inhalte kontrolliert hätten. Von der Schule wurde dieser Sachverhalt bestätigt. Ziel der Aktion sei es gewesen, Videos mit gewaltverherrlichenden bzw. nationalsozialistischen Inhalten zu finden und von den Schülern löschen zu lassen.“[13] Der Berliner Datenschutzbeauftragte kommt zu dem Ergebnis, dass nach § 64 Abs. 1 Schulgesetz für das Land Berlin (SchulG) Schulen die personenbezogenen Daten von Schülern nur erheben dürfen, die zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen „schulbezogenen“ Aufgaben erforderlich sind. Gemeint ist damit aber nicht der allgemeine Auftrag der Schule zur Bildung und Erziehung, sondern nur die „schulbezogenen“ Aufgaben, die (im engeren Sinne) mit der Organisation und Durchführung des Schulbetriebes verbunden sind. In der Kenntnisnahme und Erhebung der umfangreichen, zum Teil vertraulichen Handydaten sieht der Datenschutzbeauftragte keine der im Schulgesetz genannten „schulbezogenen“ Aufgaben. Die pädagogische Aufbereitung des Themas „Gewaltverherrlichung“ könne auch ohne die Überführung von „Einzeltätern“ erfolgen. Das Fazit aus Datenschutzsicht: „Bei den Inhaltsdaten von Schüler-Handys handelt es sich um zum Teil vertrauliche Daten des Besitzers und Dritter. Diese Daten dürfen Lehrkräfte einer Schule nur mit Einwilligung der Betroffenen erheben. Beim Verdacht der Begehung von Straftaten hat eine Mitteilung an die Strafverfolgungsbehörden zu erfolgen, die dann entsprechende Durchsuchungen der Inhaltsdaten von Handys vornehmen können.“ Diese rechtliche Würdigung fand auch die Unterstützung des Berliner Senats: „Der Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit stellt zu Recht darauf ab, dass es nach den derzeitigen gesetzlichen Bestimmungen Lehrkräften nicht erlaubt ist, die auf Schülerhandys gespeicherten Daten ohne deren Einwilligung zu durchsuchen. Liegen Anhaltspunkte für ein strafrechtlich relevantes Verhalten vor, so kann die Lehrkraft nach § 62 Abs.2 Nr. 6 SchulG das Handy einziehen und der herbeigerufenen Polizei übergeben, die dann weitere Maßnahmen veranlassen kann.“ [14]

Der „Gang zur Toilette“ – Erfassung von kurzzeitigen Abwesenheiten vom Unterricht

Nicht selten werden die Landesdatenschutzbeauftragten auf Beschwerden von Schülerinnen und Schülern tätig. So auch der Berliner Datenschutzbeauftragte, als sich eine Schülerin darüber beschwerte, dass an ihrer Schule der Gang zur Toilette während des Unterrichts von einer Lehrkraft notiert werde: „Die Namen der Schülerinnen und Schüler, die ihrem `natürlichen Bedürfnis´ nachgehen, würden in Listen erfasst. Die Listen würden in den Klassenbüchern verbleiben und erst vernichtet, wenn sie `voll´ sind. Der Sachverhalt wurde uns von der Schulleitung auf Nachfrage bestätigt. Begründet wurde die `Erfassung der Toilettengänge´ damit, dass es in der Vergangenheit mehrfach zu Sachbeschädigungen in den Toilettenräumen gekommen sei.“[15]

Für den Datenschützer gehört zu den schulbezogenen Aufgaben, die nach § 46 Abs. 2 SchulG für Schülerinnen und Schüler bestehende Verpflichtung zur verbindlichen und aktiven Teilnahme am Schulunterricht zu kontrollieren und ggf. Verstöße dagegen zu dokumentieren: „Dem entspricht § 5 Abs. 1 SchulDatenVO, wonach die Fehlzeiten von Schülerinnen und Schülern (einschließlich Verspätungen und Beurlaubungen) sowie sonstige besondere Vorkommnisse im Klassenbuch festzuhalten sind. Auch das kurzzeitige Verlassen des Unterrichts durch eine Schülerin oder einen Schüler kann daher, vergleichbar einer Verspätung, im Klassenbuch (hier: in einer Liste, die dem Klassenbuch beigelegt ist) erfasst werden.“ Allerdings ist es bei „kurzzeitigen Fehlzeiten“ ausreichend, lediglich Namen, Vornamen und die Abwesenheitszeit zu protokollieren. „Die Erfassung des Abwesenheitsgrundes (z. B. Toilettengang) ist für den genannten Zweck dagegen nicht erforderlich und damit datenschutzrechtlich unzulässig.“ Die Empfehlung aus Datenschutzsicht: „Die Vernichtung der Liste (ohne Abwesenheitsgrund) hat zeitnah (jedenfalls nicht erst, wenn sie vollgeschrieben ist), z. B. wöchentlich, zu erfolgen. (…). Kurzzeitige Abwesenheiten vom Unterricht dürfen allenfalls ohne Angabe des Grundes (z. B. Toilettenbesuch) erfasst werden. Die Verfolgung und Aufklärung von Straftaten ist originär den Strafverfolgungsbehörden vorbehalten. Eine Verarbeitung von personenbezogenen Schülerdaten zu diesem Zweck kann nicht auf § 64 Abs. 1 SchulG gestützt werden und ist unzulässig.“

Schülerdaten und -bilder im Internet

Kaum ein Tätigkeitsbericht, in dem nicht von rechtswidrigen Veröffentlichungen von Schülerdaten und -bildern im Internet durch Schulen berichtet wird. So auch im 24. Tätigkeitsbericht aus Bayern, in dem der Landesdatenschutzbeauftragte die grundsätzlichen „Spielregeln“ bei der Preisgabe von Schülerdaten zum wiederholten Male darstellt: „Für die weltweite Veröffentlichung personenbezogener Daten von Lehrkräften, Schülerinnen und Schülern, Erziehungsberechtigten und sonstigen am Schulleben Beteiligten auf der Schulhomepage – dazu gehören insbesondere auch Fotos – bedarf es grundsätzlich einer freiwilligen, informierten und schriftlichen Einwilligung des jeweiligen Betroffenen. Eine Ausnahme besteht nur hinsichtlich der dienstlichen Kommunikationsdaten (Name, Namensbestandteile, Vorname(n), Funktion, Amtsbezeichnung, Lehrbefähigung, dienstliche Anschrift, dienstliche Telefonnummer, dienstliche E-Mail-Adresse) der Schulleitung und von Lehrkräften, die an der Schule eine Funktion mit Außenwirkung wahrnehmen; lediglich insoweit ist keine Einwilligung erforderlich. Sind die Betroffenen noch minderjährig, so muss die Einwilligung bis zur Vollendung des 14. Lebensjahres durch die Erziehungsberechtigten und ab Vollendung des 14. Lebensjahres durch die Minderjährigen selbst und deren Erziehungsberechtigte erfolgen.“ [16]

Aber auch mit dem Einholen einer Einwilligung vor Veröffentlichung haben Schulen so ihre Probleme. Bei der datenschutzrechtlichen Prüfung eines städtischen Gymnasiums in München stellte die Datenschutzaufsicht fest, dass das Gymnasium lediglich im ersten Elternbrief zu Schuljahresbeginn in einem Unterpunkt auf die Veröffentlichung personenbezogener Daten auf der Schulhomepage hingewiesen und den Eltern ein befristetes Widerspruchsrecht eingeräumt hatte. Das ist keine wirksame Einwilligung im Sinne des Datenschutzrecht: „Eine solche Verfahrensweise genügt den in Art. 15 Abs. 2 bis 4, 7 BayDSG aufgestellten datenschutzrechtlichen Anforderungen an eine Einwilligung keinesfalls. Vielmehr muss eine ausdrückliche schriftliche Einwilligung eingeholt werden. Dabei sind die Betroffenen darüber zu informieren, welche personenbezogenen Daten zu welchem Zweck auf die Homepage eingestellt werden sollen. Ferner ist im Einwilligungsformular darauf hinzuweisen, dass die Einwilligung freiwillig und widerruflich ist sowie dass den Betroffenen keine Nachteile entstehen, wenn sie die Einwilligung verweigern oder widerrufen.“

In Baden-Württemberg veröffentlichten gleich mehrere Schulen vollständige Listen aller Abiturienten in Form der Teilnahmelisten an den mündlichen bzw. Präsentationsprüfungen im Internet. Ferner enthielten die Veröffentlichungen neben den Namen und Vornamen der Schülerinnen und Schüler bestimmter, auch bereits zurückliegender Abiturjahrgänge Angaben über deren jeweilige Prüfungsfächer und die Tage und Uhrzeiten, an denen bestimmte Prüfungen abzulegen waren. Auch in diesem Fall ist das Fazit eindeutig: „Eine solche weltweite Streuung personenbezogener Daten im Internet ist mit den dienstlichen Erfordernissen der Gymnasien in keiner Weise zu rechtfertigen und somit ohne die Einwilligung der betroffenen Schülerinnen und Schüler oder gegebenenfalls der jeweiligen Erziehungsberechtigten schlicht illegal.“ [17]

Gegensprechanlage mit Überwachungsmöglichkeit

Über einen ganz besonderen Datenschutzverstoß berichtet die Landesdatenschutzbeauftragte Brandenburg in ihrem 15. Tätigkeitsbericht.[18] In einer Förderschule für geistig behinderte Kinder wurde eine Gegensprechanlage installiert, die das unbemerkte Abhören der Unterrichtsräume ermöglichte. „Im Zuge des Umbaus eines Gebäudes zu einer Förderschule hat der zuständige Schulträger eine Wechselsprechanlage installiert, damit Lehrkräfte im Notfall schnell das Sekretariat alarmieren können. Es gab Grund zur Annahme, dass diese Anlage missbräuchlich genutzt werden könnte.“ Bei einem unangekündigten Kontrollbesuch stellten die Datenschützer fest, dass jede Person vom Sekretariat aus eine Verbindung zu den Nebenstellen in den Fach-, Klassen-, Aufenthalts- und Büroräumen hätte aufbauen können und so die Möglichkeit bestand, da die Nebenstellen den Aufbau einer Verbindung weder optisch noch akustisch anzeigte, Lehrer und Schüler unbemerkt abzuhören. Angesichts einer solchen technischen Konfiguration einer Wechselsprechanlage ist ein datenschutzgerechter Betrieb nicht möglich.

Der Datenschützer forderte Abhilfe; was aber nicht so leicht möglich war. „Da ein Umbau technisch ausgeschlossen war, musste eine Lösung gefunden werden, bei der die Anlage nur in einer Richtung zu betreiben ist, um das Absetzen eines Notrufes von der Nebenstelle zum Sekretariat zu ermöglichen. Nach intensiver Beratung durch unsere Behörde ist das zentrale Bedienteil in einem elektromechanisch verriegelten Kompaktschaltschrank mit manipulationssicherem Ereignisspeicher eingebettet worden. Dieser ermöglicht den Zugriff erst nach einer Authentifizierung mittels eines personalisierten Schlüssels. Der Lautsprecher wurde so angeordnet, dass der Notruf von der Nebenstelle zum Sekretariat jederzeit dort akustisch wahrgenommen werden kann. Somit können alle anwesenden Personen, auch wenn sie nicht über einen Schlüssel verfügen, entsprechende Hilfsmaßnahmen ergreifen. Da der Betrieb der Gegensprechanlage geeignet ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen, handelt es sich gem. § 65 Nr. 2 Personalvertretungsgesetz um eine mitbestimmungspflichtige Angelegenheit, bei der der Lehrerrat im Rahmen einer Dienstvereinbarung zu beteiligen ist. Diese Dienstvereinbarung muss im Wesentlichen Festlegungen zur Umsetzung der getroffenen Maßnahmen, zu Zugangsberechtigungen sowie zur Art und Weise der Auswertung der Protokolldateien enthalten. Aus unserer Sicht sind die nunmehr getroffenen technischen und organisatorischen Maßnahmen geeignet, die missbräuchliche Nutzung des unbemerkten Abhörens von Schülern und Lehrern weitestgehend zu verhindern.“

Noten im Internet

Auf einen eigentlich leicht in der Schulpraxis durch Lehrerinnen und Lehrer sowie Schulleitungen zu beherzigen einfachen Grundsatz und Dienstauftrag weist der Hamburgische Datenschutzbeauftragte in seinem 22. Tätigkeitsbericht hin: „Originäre Aufgabe der Lehrkräfte ist es, den gesetzlichen Bildungs- und Erziehungsauftrag der Schule zu erfüllen. Die hierbei anfallenden personenbezogenen Daten der Schülerinnen und Schüler dürfen aber nur im notwendigen Umfang erhoben, verarbeitet oder an andere Stellen übermittelt werden. Dies ist nicht der persönlichen Einschätzung der Lehrkräfte überlassen, sondern ergibt sich aus den Datenverarbeitungsnormen des Hamburgischen Schulgesetzes (HmbSG), das durch die Schul-Datenschutzverordnung sowie die allgemeinen Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) ergänzt wird. Den Lehrkräften sollte also diese Normendreifaltigkeit vertraut sein.“ [19] Das dies aber nicht immer der Fall ist zeigt sich in einem gravierenden Datenschutzverstoß: „Eine Lehrkraft hatte die Ergebnisse einer Klausurarbeit in das Internet eingestellt, und zwar unter Angabe der vollständigen Schülernamen, der Schüler-Identifikationsnummern und Anmerkungen zu den erzielten Leistungen.“ Der Datenschützer kam zu einem Ergebnis, zu dem eigentlich auch ein Lehrer ohne große datenschutzrechtlichen Kenntnisse kommen müsste: „Die Veröffentlichung der Daten im Internet war mithin rechtswidrig.“ Daher wurde die Lehrkraft von der Schulleitung dienstrechtlich gerügt. Aber damit hat dies Geschichte und ein weiterer im Tätigkeitsbericht beschriebener Fall

noch nicht sein Ende gefunden: „Unsere Prüfung, ob wir zusätzliche Maßnahmen gegen die Lehrkräfte einleiten, dauerte bis zum Redaktionsschluss noch an. Die Beispiele zeigen aber, dass die Vermittlung datenschutzrechtlicher Grundsätze bei den Lehrkräften noch verbesserungswürdig ist. Besonders gefordert hierbei sind die Schulleitungen und die Behörde für Schule und Berufsbildung."

Lehrerdaten auf der Schulhomepage

Ebenfalls Dauerthema in den Datenschutzberichten ist die Veröffentlichung von Lehrerdaten im Internet. Eine Variante wird im Tätigkeitsbericht für 2009 [20] des Berliner Datenschutzbeauftragten beschrieben. So erhielt er mehrere Anfragen von Schulleitungen, ob es erlaubt sei, Vertretungspläne unter Nennung des konkreten Namens des Vertreters bzw. des Vertretenen ins Internet zu stellen. In seiner Antwort weist der Datenschützer darauf hin, dass Personaldaten aufgrund der besonderen Gefährdung des informationellen Selbstbestimmungsrechts der Beschäftigten bei einer (weltweiten) Veröffentlichung ihrer Daten nur unter Berücksichtigung der erforderlichen Sorgfalt und Erforderlichkeit ins Internet gestellt werden dürfen: „Es besteht weder eine vertragliche noch eine dienstrechtliche Duldungspflicht der Beschäftigten zur Aufnahme dieser Daten in das Internet. Die Einholung eines Einverständnisses ist in Dienst- und Arbeitsverhältnissen regelmäßig datenschutzrechtlich unzureichend, da aufgrund der bestehenden Abhängigkeit der Beschäftigten zum Dienstherrn und Arbeitgeber eine derartige Erklärung häufig nicht freiwillig ist. Die Freiwilligkeit ist jedoch Voraussetzung für ein wirksames Einverständnis."

Sensibles Schriftgut an Schüler verteilt

Unter der Überschrift „Sparsamkeit am falschen Platz: Datenschutz an einer Gesamtschule" berichtet der Landesdatenschutzbeauftragte von Baden-Württemberg[21] über den Fall einer Lehrerin, die nicht „nur" aus Nichtwissen, sonder vorsätzlich gegen den Schutz von vertraulichen Schüler- und Elterndaten verstieß: „Besorgte Eltern von Schülern einer Gesamtschule haben sich an mein Amt gewandt und mitgeteilt, eine Lehrkraft dieser Schule habe ihren Schülern Kopien des Lehrplans für Geschichte ausgeteilt. Sie habe der Klasse zuvor erklärt, dass sie für Kopien – aus Gründen der Sparsamkeit und des Umweltschutzes – stets bereits einseitig bedrucktes Papier aus dem Mülleimer des Kopierraums verwenden würde. Dabei habe sie betont, dass möglicherweise auch dem Datenschutz unterliegende Kopien dabei seien, die die Schüler wieder zurückgeben könnten. Und tatsächlich hat die Lehrerin Schreiben an Eltern über störendes Verhalten einzelner, namentlich genannter Schüler \`wiederverwendet´. Die Namen von Eltern und Schülern waren dabei so unzureichend geschwärzt, dass die Namen der Betroffenen ohne Weiteres zu lesen waren. Auf diese Weise seien, so teilten die Eltern mit, persönliche Mitteilungen der Schulleitung an einzelne Eltern zum Verhalten ihrer Kinder weitergegeben worden, wobei Name und Anschrift der Erziehungsberechtigten und der Kinder erkennbar gewesen seien."

Auf die mehrmalige Nachfrage des Datenschutzbeauftragten wurde der von den Eltern beschriebene Sachverhalt durch die Schule bestätigt, wobei aber eine „Rechtfertigung" vorgetragen wurde: „Allerdings sei die Lehrerin der Auffassung gewesen, es sei ausreichend, die Adressen zu schwärzen; dabei habe sie versäumt, die Wirksamkeit des Schwärzens zu überprüfen. Zudem sei die Lehrkraft davon ausgegangen, es genüge, Oberstufenschüler darauf hinzuweisen, dass Blätter mit erkennbaren personenbezogenen Daten Dritter von den Schülern zurückzugeben seien." Die Schule teilte aber auch mit, es sei im Kollegium üblich, Schreiben mit personenbezogenen Daten, die keine Verwendung mehr fänden, zerrissen und weggeworfen würden. Ferner werde im Sekretariat oder bei der Schulleitung nicht benötigtes Schriftgut in einem Reißwolf vernichtet. Der Datenschützer dazu: "Bei den Angaben auf den Elternbriefen handelte es sich um besonders sensible personenbezogene Daten, die unter anderem die Verhaltensauffälligkeiten einiger Schüler beschreiben. Der Umgang mit solchen Daten stellt hohe Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen. Die an der Schule getroffenen organisatorischen Regelungen waren ganz offensichtlich nicht ausreichend: Die Lehrkraft hatte nur unzureichende Maßnahmen zur Unkenntlichmachung personenbezogener Daten ergriffen. Es genügte auch nicht, die Schüler aufzufordern, Papier mit personenbezogenen Daten Dritter zurückzugeben. Ungeachtet der Frage, ob die Lehrerin davon ausgehen konnte, dass die Schüler ihrer Aufforderung, entsprechende Papiere zurückzugeben, nachkommen, nahm sie in Kauf, dass die Schüler – und damit Unbefugte – diese Daten einsehen konnten. Der Umstand, dass Unterlagen mit solch sensiblen personenbezogenen Daten in einem Papiermülleimer gelandet sind, belegt, dass auch anderen Lehrkräften der Schule ein korrekter Umgang mit Schriftgut nicht bekannt war. Auch die Darstellung der Schule, wonach es im Kollegium üblich sei, nicht mehr benötigtes Schriftgut mit personenbezogenen Daten unter anderem durch \`Zerreißen´ zu vernichten, zeigt grundsätzliche datenschutzrechtliche Defizite im Schulbetrieb auf. Allein durch das manuelle Zerreißen von Schriftstücken kann nicht wirksam verhindert werden, dass Unbefugte auf Daten zugreifen." Sonderlich lernbereit zeigte sich die Schulleitung auf die Hinweise allerdings nicht: "Zwar hat die Schule mitgeteilt, dass die Vorgehensweise der Lehrkraft falsch gewesen und diese belehrt worden sei. Jedoch sind faktisch sensible personenbezogene Daten von Schülern durch mangelhafte organisatorische Kontrollen in die Hände unbefugter Dritter gelangt. Zudem hat die Schule nicht mitgeteilt, dass die bereits in der Vergangenheit im Rahmen von Gesamtlehrerkonferenzen durchgeführten Belehrungen erweitert oder konkretisiert worden seien. Insofern konnte an dieser Schule der datenschutzgerechte Umgang mit Schriftstücken, die personenbezogene Daten enthalten, offenbar nicht ausreichend gewährleistet werden. Eine Beanstandung war die zwangsläufige Folge."

Erhebung von Gesundheitsdaten

Nicht selten wird in den Tätigkeitsberichten über den datenschutzwidrigen Umgang mit Gesundheitsdaten von Schülerinnen und Schülern durch einzelne Lehrkräfte oder Schulleitungen berichtet. So erörtert der Sächsische Datenschutzbeauftragte in seinem 15. Tätigkeitsbericht[22] die Frage, inwieweit die Forderung der Schule nach Angabe eines Grundes bei Sportbefreiung oder bei Verhinderung der Teilnahme am Unterricht rechtmäßig ist: „Ein seltsames Beispiel war das Verlangen eines Sportlehrers einer Mittelschule. Dieser beabsichtigte zur Sicherstellung der Teilnahme am Sportunterricht eine Liste zu erstellen, aus der hervorgehen sollte, wann die Schülerinnen der Klasse menstruationsbedingt dem Sportunterricht fernblieben. Aber auch andere Eltern führten in anderen Fällen aus, dass sie von der Schule ihres Kindes informiert worden seien, dass bei Krankheit zukünftig zwingend eine Bescheinigung vorzulegen wäre, aus der der Grund der Erkrankung ersichtlich sein müsste. Die datenschutzrechtliche Überprüfung dieser Anforderung der Schule ergab, dass die Forderung der Schule nach der Mitteilung des Grundes der Erkrankung (im Sinne einer Diagnose) rechtswidrig gewesen war. Nach § 4 Abs. 1 Sächsisches Datenschutzgesetz (SäDSG) darf die Schule als öffentliche Stelle personenbezogene Daten verarbeiten, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt. Das Erheben personenbezogener Daten ist dabei nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist (§ 12 SächsDSG). Zur Teilnahme am Unterricht regelt § 1 SBO, dass die Schüler an öffentlichen Schulen im Sinne von § 3 Abs. 2 SchulG zur pünktlichen und regelmäßigen Teilnahme am Unterricht und an vom Schulleiter für verbindlich erklärten Schulveranstaltungen verpflichtet sind. Ist ein Schüler durch Krankheit oder aus anderen nicht vorhersehbaren zwingenden Gründen verhindert die Schule zu besuchen, so ist dies der Schule unter Angabe des Grundes und der voraussichtlichen Dauer der Verhinderung unverzüglich mitzuteilen (§ 2 SBO). Bei einer Krankheitsdauer von mehr als fünf Tagen sowie bei Teilzeitunterricht von mehr als zwei Unterrichtstagen kann der Klassenlehrer oder der Tutor vom Entschuldigungspflichtigen die Vorlage eines ärztlichen Zeugnisses verlangen. Bei der Information ‚Angabe des Grundes' im Sinne der Schulbesuchsordnung handelt es sich lediglich um allgemeine Angaben, z. B. ‚krankheitsbedingt' oder aus ‚gesundheitlichen Gründen'. Darüber hinausgehende Daten zum gesundheitlichen Zustand eines Schülers ist die Schule nicht zu erheben befugt."

Allerdings ist in speziellen Fällen Schulen die Erhebung und Speicherung auch von Gesundheitsdaten aufgrund des Sächsischen Schulgesetzes und entsprechender Verwaltungsvorschriften erlaubt. In der ausführlichen Darstellung dazu heißt es u.a.: „Die Speicherung von Gesundheitsdaten im schulischen Bereich ist mit der Einwilligung der Eltern oder bei volljährigen Schülern und Auszubildenden mit deren Einwilligung jedoch möglich. Dazu regeln die jeweils geltenden Schulordnungen, dass z. B. eine durch dafür qualifizierte Lehrer oder Schulpsychologen festgestellte Teilleistungsschwäche, Art und Grad einer Behinderung oder chronischen Krankheit, soweit sie für den Schulbesuch oder die Ausbildung von Bedeutung sind, durch die Schule gespeichert werden dürfen. Zumeist werden diese Angaben bereits nach den Verordnungen der einzelnen Schulrichtungen bei der Schulaufnahme erhoben und sie werden als Informationen von den Elternsorgeberechtigten an die Schule gegeben. Als ein Beispiel, in dem die Kenntnis von solchen Daten sinnvoll ist, sei die Kenntnis des Sportlehrers von chronischen Erkrankungen genannt, die er im Rahmen des regulären Sportunterrichts beachten muss."

Auch wird die Frage erörtert, ob die Erhebung der Krankenkassendaten von Schülern allgemein und wegen der durchzuführenden Klassenfahrten zulässig sei. Ergebnis: „Die Angabe der Krankenkasse, der Krankenkassennummer und weiterer Angaben sind nur beim Eintritt eines Krankheitsfalles oder bei Unfällen erforderlich. Eine Erfassung der Daten in der Schülerakte, in Dateien oder im Notenbuch ist nicht erforderlich. Bei einem Unfall und im Krankheitsfall sind die Elternsorgeberechtigten zu benachrichtigen, die die erforderlichen Krankenkassenangaben machen können. Sofern eine Gesundheitsgefahr für den Schüler abgewendet werden muss, können medizinische Maßnahmen ohnehin bereits ohne die Elternsorgeberechtigten eingeleitet werden und es ist nach den Regeln der mutmaßlichen Einwilligung zu verfahren."

Weitergabe von Schülerdaten zu Werbezwecken

Ausführlich geht der Bayerische Landesdatenschutzbeauftragte in seinem 24. Tätigkeitsbericht[23] auf die Weitergabe von Schülerdaten zu Werbezwecken ein. Gleich in mehreren Fällen wurde er darauf aufmerksam, dass Daten und Unterlagen über Schülerinnen und Schüler sowie deren Erziehungsberechtigte von Schulen an außerschulische Stellen für kommerzielle Zwecke weitergegeben wurden: „Dabei macht es keinen Unterschied, ob die Schulen die Daten selbst weitergeben oder ob sie Datenerhebungen durch außerschulische Stellen – oftmals getarnt als Geschenkauslobungen oder (Wissens-)Wettbewerbe – in der Schule dulden. Aufgefallen in diesem Zusammenhang sind mir vor allem Kreditinstitute, Krankenkassen und (Buch-)Direktvertriebsunternehmen, aber auch nichtgewerbliche Akteure wie beispielsweise Musikchöre, die an Schulen um neue Mitglieder werben."

Als besonders anschauliches Beispiel wird folgender Sachverhalt beschrieben: „Die Erziehungsberechtigten eines ABC-Schützen haben mich darüber informiert, dass die Eltern aller künftigen Schulanfänger noch vor dem ersten Schultag persönlich adressierte Anschreiben der örtlichen Sparkasse erhalten hatten. In diesen Schreiben hatte die Sparkasse Glückwünsche zur Einschulung des Kindes übermittelt und eine – persönlich von Sparkassenmitarbeitern in der Schule zu überreichende – Trinkflasche ausgelobt. `Daneben´ hatte die Sparkasse auf die Bedeutung des richtigen Umgangs mit Geld hingewiesen und insoweit sogleich ihre Beratung angeboten. Die für die Anschreiben erforderlichen Adress- und Namensdaten

der Erziehungsberechtigten der künftigen Schulanfänger hatte die Sparkasse von der Grundschule erhalten." Der Datenschutzbeauftragte weist darauf hin, dass nach den in Bayern geltenden Vorschriften den Schulen die Weitergabe von Daten und Unterlagen über Schülerinnen und Schüler und Erziehungsberechtigte an außerschulische Stellen nicht erlaubt ist. Ein Ergebnis, zu dem auch die datenschutz- und schulrechtlichen Regelungen in den anderen Bundesländern führen. Ausnahmen gelten nur für die Fälle, in denen die Weitergabe zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben ausdrücklich erlaubt ist. Der Datenschutzbeauftragte erinnert die Verantwortlichen an die „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes"[24], wonach es den Schulen verboten ist, Schülerdaten zu Werbezwecken weiterzugeben: „Diese Bestimmung korrespondiert mit dem in Art. 84 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) vom bayerischen Gesetzgeber aufgestellten Verbot der kommerziellen Werbung an Schulen. So sind nach Art. 84 Abs. 1 BayEUG der Vertrieb von Gegenständen aller Art, Ankündigungen und Werbung hierzu, das Sammeln von Bestellungen sowie der Abschluss sonstiger Geschäfte in der Schule grundsätzlich untersagt."

Fazit: „In dem von mir eingangs herausgegriffenen Beispielsfall war die Übermittlung der Schülerdaten durch die Grundschule an die örtliche Sparkasse weder zur Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich, noch hatte die Sparkasse einen rechtlichen Anspruch auf die Herausgabe dieser Daten. Ich habe die Schule daher darauf hingewiesen, dass die Datenübermittlung unzulässig war. Die Grundschule hat unverzüglich ihren Fehler eingeräumt und mir für die Zukunft die genaue Beachtung der schul- und datenschutzrechtlichen Vorgaben zugesichert."

Videoüberwachung an Schulen

Nicht nur im öffentlichen Raum werden zunehmend Videokameras eingesetzt, sondern auch in Schulen. Hatte das Bildungsministerium Rheinland-Pfalz im Jahr 2004 keine Kenntnis von Videokameras im Schulbereich, ergab eine Umfrage des Landesbeauftragte für den Datenschutz Rheinland-Pfalz (LfD) im Jahr 2008, dass an 85 Schulen insgesamt 193 Kameras im Einsatz waren: „Da die Rücklaufquote nur bei ca. 68 Prozent lag, muss von einer noch größeren Anzahl von Videoüberwachungsmaßnahmen im Schulbereich ausgegangen werden. Auffällig war, dass sich der Kameraeinsatz nicht nur auf die Außenbereiche (Schulhof, Fahrradabstellplätze) beschränkt, sondern auch im Innenbereich eine Überwachung selbst von solch sensiblen Bereichen wie z.B. Lehrerzimmer, Sekretariatseingang oder Toiletten stattfindet. Eine Schule beklagte sich kurioserweise sogar darüber, dass die Videokamera bei einem Einbruch entwendet wurde."[25] Die Umfrage ergab darüber hinaus, dass den gesetzlichen Voraussetzungen des § 34 LDSG in der Praxis vielfach nicht Rechnung getragen wird. So wurde z.B. die gesetzlich vorgeschriebene Kennzeichnung der Videoüberwachung unterlassen und die aufgezeichneten Daten zu lange gespeichert. Der LfD nahm das nicht sonderlich erfreuliche Ergebnis zum Anlass eine „Orientierungshilfe zur Zulässigkeit von Videoüberwachungsmaßnahmen im Schulbereich"[26] zu erstellt.

Videokamera im Warteraum des schulpsychologischen Dienstes

Oft werden die Datenschutzbehörden erst eingeschaltet, wenn es zu einer Datenschutzpanne gekommen ist. Da ist es schon besser, vor Umsetzung von datenschutzrelevanten Maßnahmen um Beratung nachzusuchen. Von so einem Fall berichtet der neue Tätigkeitsbericht[27] aus dem Saarland: „Ein schulpsychologischer Dienst überlegte, in seinem Warteraum eine Videokamera zu installieren. Dies vor dem Hintergrund, dass im Rahmen schulpsychologischer Untersuchungen Elterngespräche ohne Anwesenheit der Kinder geführt werden und dass diese sich in dieser Zeit allein im Wartezimmer aufhalten. Besonders unruhige oder verhaltensauffällige Kinder benötigten hierbei Beaufsichtigung. Da eine Beaufsichtigung durch die Mitarbeiterin des Geschäftszimmers nicht immer sichergestellt werden könne, halte man die Anbringung einer Videokamera für eine gute Lösung. Mein Vorgänger hat demgegenüber darauf hingewiesen, dass jede Form der Videoüberwachung einen Eingriff in das Persönlichkeitsrecht der davon betroffenen Personen darstellt, der nur zulässig ist, wenn es hierfür eine gesetzliche Grundlage gibt. Vorliegend sollte eine Videoüberwachung in nicht öffentlich zugänglichen Räumen erfolgen, so dass die Zulässigkeit der Maßnahme nach allgemeinem Datenschutzrecht zu beurteilen war. Die Zulässigkeit der Videoüberwachung hängt nach dessen Vorschriften von der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der Maßnahme ab.

Dem schulpsychologischen Dienst wurde mitgeteilt, dass unter Zugrundelegung dieser Maßstäbe eine Überwachung des Warteraumes datenschutzrechtlich bedenklich ist. Unverhältnismäßig ist eine Überwachung auf jeden Fall, wenn sich auch Erwachsene in dem Raum aufhalten. Abgesehen davon, dass es in diesem Fall keinen Grund für eine Überwachung gibt, würden die Betroffenen unverhältnismäßig belastet, indem sie sich einer ständigen Überwachungssituation ausgesetzt sehen. Keine praktikable Lösung wäre es, die Mitarbeiterin der Geschäftsstelle anzuweisen, die Videokamera nur einzuschalten, wenn sich unruhige oder verhaltensauffällige Kinder allein in dem Raum aufhalten. Denn einerseits besteht die Gefahr, dass die Kamera doch permanent eingeschaltet bleibt. Zu berücksichtigen ist aber vor allem, dass die Videokamera sichtbar ist und ein entsprechendes Schild auf die Videoüberwachung hinweist, so dass für einen wartenden Erwachsenen nicht erkennbar wäre, ob die Anlage eingeschaltet ist oder nicht. Zweifel sind auch angebracht, ob eine Videokamera überhaupt geeignet ist, den mit ihr verfolgten Zweck zu erreichen. So ist fraglich, ob die Mitarbeiterin des Geschäftszimmers den Bildschirm neben ihren sonstigen Arbeiten permanent so im Blick haben kann, dass sie im Ernstfall schnell genug reagieren kann, um einen Schaden abzuwenden. Überlegenswert ist, ob es nicht andere Maßnahmen gibt, um eine effektive Aufsicht zu gewährleisten. Zu denken wäre hier an eine Gestaltung der Räumlichkeiten, die es der Mitarbeiterin

in der Geschäftsstelle ermöglicht, wartende Kinder im Auge zu behalten. Eine andere Möglichkeit wäre auch, die Kinder im Geschäftszimmer warten zu lassen, zumal es wohl nicht sinnvoll ist, verhaltensauffällige Kinder längere Zeit in einem separaten Warteraum alleine zu lassen. Der schulpsychologische Dienst hat daraufhin mitgeteilt, dass er aufgrund der von mir vorgebrachten Bedenken auf die Installation einer Videokamera in seinem Warteraum verzichtet."

„Offene Mathe-Foren" an einem Gymnasium

Einen ganz besonderen Fall von Datenschutz-Ignoranz schildert der Landesdatenschutzbeauftragte in Baden-Württemberg in seinem 29. Tätigkeitsbericht[28]: „Es begann damit, dass mein Amt durch besorgte Eltern auf ein sog. `Mathe-Forum´ an einem Gymnasium angesprochen wurde. Dabei mussten, so hieß es, Schülerinnen und Schüler von insgesamt vier Klassen benotete Mathematik-Übungen machen. Wer sich nicht daran halte und nicht wöchentlich teilnehme, bekomme eine schlechte Benotung. Meine Mitarbeiter gingen der Sache sogleich nach und mussten feststellen, dass im Internet-Angebot des Gymnasiums zu den dort betriebenen `Mathe-Foren´ eine Vielzahl von Namen, insbesondere von Schülerinnen und Schülern, und diesen zuordenbare weitere Angaben frei abrufbar waren. Somit konnte weltweit jeder, der über einen Internet-Zugang verfügt, lesen, wie sich welche Gymnasiasten und punktuell auch die Lehrkraft mit Blick auf die Mathematikaufgaben äußerten. Dabei ergab sich, wie stets im realen Leben, kein Bild problemloser und perfekter Bewältigung der Aufgaben. Es drängten sich in einigen Fällen – stets auf die mit vollem Namen genannten Gymnasiasten beziehbar – vielmehr die heiklen Fragen auf, ob denn alle Aufgaben mit dem nötigen Engagement, Ernst und Sachverstand bearbeitet werden oder ob hier Defizite zu beklagen sind. Daraufhin bat mein Amt die Schule rasch um kurzfristige Stellungnahme zu den hier eingegangenen Mitteilungen sowie zum Ergebnis unserer eigenen Internet-Recherche und wies zudem darauf hin, dass die Schule gegebenenfalls eine nun selbst als rechtswidrig erkannte Datenverarbeitung unverzüglich zu beenden hat." Die Schule reagierte prompt auf dem Hinweis durch den Datenschützer und stellte das datenschutzrechtlich illegale „Mathe-Foren" sofort ab. Allerdings verlief die Angelegenheit dann doch nicht so erfreulich: „Unerfreulich und besorgniserregend war dagegen, dass die Schule, auch in den späteren Äußerungen des Schulleiters, ein tiefgreifendes Unverständnis für datenschutzrechtliche Anforderungen und somit gravierende Defizite und Probleme erkennen ließ. Jedenfalls war der dringende Beratungs- und Kontrollbedarf augenfällig und führte zu einem Vor-Ort-Termin an der Schule. Die eingehende Beratung durch meine Mitarbeiter fiel allerdings beim Schulpersonal auf unfruchtbaren Boden. Die Schulleitung äußerte zwar wiederholt, auch unter Hinweis auf die einschlägige Verwaltungsvorschrift des Kultusministeriums zur Verarbeitung personenbezogener Daten durch öffentliche Schulen, dass man den Datenschutz als wichtig betrachte und ernst nehme. Im Gesamtbild erwiesen sich diese Worte leider als bloße Lippenbekenntnisse. Zur Erklärung wurde mehrfach geltend gemacht, dass die Verwaltungsvorschrift des Kultusministeriums unverständlich und somit für die Schule nicht hilfreich sei. So verwundert es nicht, dass der Schulleiter sich kaum um diese `Mathe-Foren´ und deren datenschutzrechtliche Zulässigkeit gekümmert und stattdessen auf die Aussage der zuständigen Lehrkraft verlassen hatte, dass `alles in Ordnung´ sei. Im Hinblick auf die Vorbildfunktion, die Lehrkräfte gegenüber den Schülerinnen und Schülern auch in Sachen des Datenschutzes haben, war das offen erkennbare Desinteresse des Schulleiters weder verständlich noch akzeptabel."

Fazit: Nachsitzen für den Datenschutz angesagt

Die beschriebenen Fälle stellen nur eine kleine Auswahl aus den in den Tätigkeitsberichten der Datenschutzbehörden beschriebenen Sachverhalten dar. Die Gesamtschau fördert ein nicht gerade ermutigendes Verhältnis und Bewusstsein der Verantwortlichen in Sachen Datenschutz an Schulen zu Tage. Das verwundert umso mehr, da nicht nur gesetzeskonformes Handeln verweigert wird, sondern auch ein wichtiges Segment des Bildungsauftrages nachlässig bis nicht wahrgenommen wird: Die Förderung, Vermittlung, Umsetzung und Wahrnehmung der für ein demokratisches Gemeinwesen unverzichtbaren Persönlichkeits- und Datenschutzrechte. Nachsitzen für Lehrkräfte und Schulleitungen in Sachen Datenschutz ist also angesagt. Die Lektüre der Tätigkeitsberichte der Datenschutzbeauftragten ist eine gute Hilfe bei der gesetzeskonformen Umsetzung des Datenschutzes. Die Fehler anderer (und die eigenen) sind ja bekanntlich nicht die schlechteste Lerngelegenheit für zukünftig richtiges Handeln. Die Landesdatenschutzbeauftragten werden so zukünftig auch die Gelegenheit erhalten, über Fälle von „best practice" im Datenschutz an Schulen zu berichten.

1 Breiter, Andreas; Welling, Stefan; Stolpmann, Björn-Eric; Medienkompetenz in der Schule – Integration von Medien in den weiterführenden Schulen in Nordrhein-Westfalen, Kurzfassung der Untersuchung im Auftrag der Landesanstalt für Medien Nordrhein-Westfalen (LfM); November 2010.

2 Vgl. Pressemitteilungen der LfM vom 22.11.2010 zur Studie „Medienkompetenz in der Schule".

3 So der Niedersächsische Landesdatenschutzbeauftragte in seinem 20. Tätigkeitsbericht (TB) (2009/2010), Landtags-Drucksache 16/4240 vom 8.12.2011, Seite 16.

4 Alle seit 1971 erschienen Tätigkeitsbericht der Aufsichtsbehörden für den Datenschutz können über das Internetportal www.zaftda.de der Technischen Hochschule Mittelhessen (THM) abgerufen werden.

5 29. TB des Landesbeauftragten für den Datenschutz in Baden-Württemberg (2008/2009), Landtags-Drucksache 14/5500 vom 1.12. 2009, Seite 66.

6 22. TB des Hamburgischen Datenschutzbeauftragten (2008/2009), Landtags-Drucksache 19/4299 vom 7.04.2010, Seite 59.

7 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.),

Praxishandbuch Schuldatenschutz, 2. überarbeitete Auflage mit neuer Datenschutzverordnung-Schule, Kiel 2009/10. Das Praxisbuch ist abrufbar über www.datenschutzzentrum.de/schule/praxishandbuch-schuldatenschutz.pdf.

8 Hessischer Datenschutzbeauftragter (Hrsg.), Datenschutz in Schulen – Überblick und Materialien zur Durchführung des Datenschutzes in Schulen, Wiesbaden 2010. Der Ratgeber und weitere Unterlagen sind abrufbar über: www.datenschutz.hessen.de/ft-schulen.htm.

9 Siehe Beitrag „BvD-Initiative: Datenschutz geht zur Schule" in dieser DANA.

10 Siehe unter www.datenschutz.rlp.de/de/jugend.php?submenu=schule.

11 Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation".

12 Siehe z.B. NRW: Bildungsportal, www.schulministerium.nrw.de/BP/Lehrer/Datenschutz.html; Baden-Württemberg: LehrerInnen-Fortbildungs-Server, http://lehrerfortbildung-bw.de/sueb/recht/ds_neu; Bayern: Staatsinstitut für Schulqualität und Bildungsforschung (ISB), www.datenschutz-schule-bayern.de.

13 Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2006, Senats-Drucksache 16/0772 vom 13.08.2007, Seite 135.

14 aaO, Seite 135.

15 Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit (2010) vom 30. März 2011, Seite 144.

16 24. TB (2009/2010) des Bayerischen Landesbeauftragten für den Datenschutz vom 1. Februar 2011, Seite 163.

17 29. TB des Landesbeauftragten für den Datenschutz in Baden-Württemberg (2008/2009), Landtags-Drucksache 14/5500 vom 1.12.2009, Seite 69.

18 15. TB der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) in Brandenburg (2008/2009), Landtags-Drucksache 5/714 vom 23. März 2010, Seite 108.

19 22. TB des Hamburgischen Datenschutzbeauftragten (2008/2009), Landtags-Drucksache 19/4299 vom 7.04.2010, Seite 59.

20 Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2009, Senats-Drucksache 16/3377 vom 2.07.2010, Seite 105.

21 30. TB Baden-Württemberg (2009/2010) vom 12.12.2011, Seite 135.

22 15. TB Sächsischer Datenschutzbeauftragter (2009/11), Landtags-Drucksache 5/7748 vom 16.12.2011, Seite 113.

23 24. TB Bayerische Landesbeauftragte für den Datenschutz (2009/10) vom 1.02.2011, Seite 167.

24 Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus und Wissenschaft, Forschung und Kunst vom 19.04.2001, KWMBl S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl S. 354.

25 22. TB Landesbeauftragter für den Datenschutz Rheinland-Pfalz (2007/09), Landtags-Drucksache 15/4300 vom 5.03.2010, Seite 77.

26 Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Orientierungshilfe für die Videoüberwachung an und in Schulen, Juni 2011, abrufbar über www.datenschutz.rlp.de/downloads/oh/oh_vue_schulen.pdf

27 23. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Saarland (2009/10), Landtags-Drucksache 14/425 vom 13.04.2011; Seite 86.

28 29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg (2008/2009), Landtags-Drucksache 14/5500 vom 1.12. 2009, Seite 66.

Aus dem 20. Tätigkeitsbericht (2009/2010) des Landesdatenschutzbeauftragten Niedersachsen, Seite 16 – Medienkompetenz:

Schüler für Datenschutz sensibilisieren!

Zur Entwicklung und Stärkung der Medienkompetenz insbesondere von Schülerinnen und Schülern haben das Land Niedersachsen und die Niedersächsische Landesmedienanstalt (NLM) das Portal „Medienkompetenz-Niedersachsen.de" erstellt, das die vorhandenen Internetplattformen zur Medienbildung und Medienerziehung vernetzt. Darin spielt der Datenschutz leider nur eine untergeordnete Rolle. Auch aus diesem Grund geben die Datenschutzbeauftragten des Bundes und der Länder Materialien, Broschüren und Orientierungshilfen heraus und führen Informationsveranstaltungen durch, um das Bewusstsein für das Recht auf informationelle Selbstbestimmung als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker zu fördern.

So hat 2010 zum Beispiel die Initiative „Klicksafe.de" in Zusammenarbeit mit einigen Datenschutzbeauftragten ein Zusatzmodul zu dem Lehrerhandbuch „Knowhow für junge User" erstellt, das unter dem Titel „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web" auf ihrer Internetseite heruntergeladen werden kann. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat eine Broschüre mit dem Titel „Meine Daten kriegt ihr nicht!" herausgegeben.

Ergänzende Informationen sind auf der Linkliste der Arbeitsgruppe „Schule/Bildung" der Datenschutzbeauftragten des Bundes und der Länder zu dem Themenschwerpunkt „Medienkompetenz und Datenschutz" zu finden. Daneben gibt es auch private Organisationen, die sich mit dem Thema Medienkompetenz befassen, wie zum Beispiel in Hannover „Smiley – Verein zur Förderung der Medienkompetenz in der Arbeit mit Kindern und Jugendlichen e. V." (www.smiley-ev.de).

Weitere Informationen:
„Meine Daten kriegt ihr nicht": www.hamburg.de/datenschutz
Linkliste: http://www.datenschutz.rlp.de/de/linkliste_ag_schule.php

Übersicht über die in den aktuell erschienen Tätigkeitsberichten der Landesdatenschutzbeauftragten erörterte Datenschutzfälle an Schulen.
Alle Tätigkeitsberichte können über www.zafda.de abgerufen werden.

Land	TB	Thema (Überschriften aus den TB)	Seite
Baden-Württemberg	30. TB 2009/10	Aktuelle Entwicklungen im Bereich der öffentlichen Schulen in Baden-Württemberg: Es tut sich etwas!	132
		Sparsamkeit am falschen Platz: Datenschutz an einer Gesamtschule	133
Bayern	24. TB 2009/10	Und nochmals: „eGovernment-Projekt“ Amtliche Schuldaten	161
		Nochmals: Internetauftritt von Schulen	162
		Passwortgeschützte Lernplattformen wie "BayernMoodle"	165
		Weitergabe von Schülerdaten zu Werbezwecken	167
		Meldungen von Erkrankungen an der Neuen Grippe durch Schulen	169
		Datenschutz beim "Nationalen Bildungspanel"	170
Berlin	32. TB 2010	Automatisierte Schülerdatei	140
		Bitte lächeln! – Weitergabe von Adressdaten an den Schulfotografen	141
		Der „Gang zur Toilette“ – Erfassung von kurzzeitigen Abwesenheiten vom Unterricht	143
		Forschungsprojekt „Jugendliche als Opfer und Täter von Gewalt“	146
Brandenburg	15. TB 2008/09	Novellierung der Datenschutzverordnung Schulwesen zur Umsetzung des Brandenburgischen Schulgesetzes	105
		Sprachstandsfeststellung vor der Einschulung	107
		Gegensprechanlage mit Überwachungsmöglichkeit	108
Bremen	33. TB 2010	Richtlinien zur Führung von Schullaufbahnakten	47
		Veröffentlichung von Schülerdaten und Fotos über Schülerinnen und Schülern im Internet	47
Hamburg	22. TB 2008/09	Videoüberwachung in Schulen	55
		Regionale Beratungs- und Unterstützungsstellen (REBUS)	56
		Zentrales Schülerregister	57
		Zusammenarbeit mit der Behörde für Schul- und Berufsbildung (BSB)	58
		Datenschutz in den Schulen	59
Hessen	39. TB 2010	Änderung des Hessischen Schulgesetzes	49
		Schwarze Listen über Lehrer	50
		Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz von Lehrkräften	51
		Beratung von Schulträgern bei der Einrichtung von Informationstechnik	53
Mecklenburg-Vorpommern	8. TB 2008/09	Forschungsvorhaben zum Krankenstand bei Lehrern	83
Niedersachsen	20. TB 2009/10	Medienkompetenz: Schüler für Datenschutz sensibilisieren!	16
Nordrhein-Westfalen	20. TB 2009/10	Datenverarbeitung durch Schule und Schulträger	96
		Datenverarbeitung durch externe Unternehmen	99
		Befragung von jugendlichen Schülerinnen und Schülern durch Jugendämter zur Lebenssituation und zum Freizeitverhalten	101
Rheinland-Pfalz	22. TB 2007/09	Schulregelungen	77
		Videoüberwachung an Schulen	77
		Online-Vertretungspläne	77
		Agentur für Qualitätssicherung (AQS)	78
		Pädagogische Netzwerke in Schulen	79
		Bildungsberichterstattung und Schulstatistik	80
Saarland	23. TB 2009/10	Aufzeichnung von Drohanrufen in saarländischen Schulen	80
		Behördliche Datenschutzbeauftragte an Schulen	81

Saarland	23. TB 2009/10	Online Noten- und Klassenbuch	82
		Einführung der Schulbuchausleihe im Saarland	83
		Vergleichsstudien an saarländischen Schulen	85
		Videokamera im Warteraum des schulpsychologischen Dienstes	86
Sachsen	15. TB 2009/11	Erhebung von Gesundheitsdaten durch die Schule – Forderung nach Angabe von Hinderungsgründen bei Sportbefreiung oder bei Allgemeinunterricht	113
		Internetpräsenzen von Schulen und erforderliche Einwilligungen	116
		Neuartige Unterrichtsmethoden und Möglichkeiten der Überwachung des Nutzerverhaltens der Schüler während des Lehrbetriebs in der Schule	117
		Datenübermittlungen von Schulen an andere öffentliche und nicht-öffentliche Stellen	119
		Videoüberwachung und Webcams im Schulbereich	120
Sachsen-Anhalt	10. TB 2009/11	Soziale Netzwerke	152
		Medienkompetenz und Datenschutzbewusstsein	152
		Prüfung in Schulen	154
		Schulverwaltungssoftware	154
		Projekt „Terminkalender für Schülerinnen und Schüler“	155
		Datenübermittlungen von Schulen an Sportvereine	156
Schleswig-Holstein	33. TB 2010	Vermittlung von Medienkompetenz – mit dem ULD	65
		Elektronische Lernplattformen und der Datenschutz	66
		LanBSH und geplanter USB-Stick erhöhen Datensicherheit	66
		Schulleiterfortbildungen im Datenschutz weiterhin erforderlich	67
		Schulen brauchen ein einheitliches und nachhaltiges Datenschutzkonzept	68
		Fehlende Umsetzung einer Meldevorschrift	69
		Schulsozialarbeit – eine prinzipiell gute Sache	69
Thüringen	8. TB 2008/09	2. Europäischer Datenschutztag mit Folgen	110
		Kooperationsvertrag TLfD/ThILLM: Ein Erfolgsmodell	110
		Der gläserne Schüler	111
		Befragung von Kindern und Jugendlichen der Stadt Jena	112



Hajo Köppen

Datenschutz an Schulen: Vorsicht ist besser als Nachsicht – Hilfe gibt es bei den Landesdatenschutzbeauftragten

Die Landesdatenschutzbeauftragten sind zuständig für die Datenschutzaufsicht in den Schulen des jeweiligen Bundeslandes. So heißt es etwa im § 25 Hessisches Datenschutzgesetz (HDSG): „Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen.“ Für eine wirksame Umsetzung dieser Kontroll- und Überwachungsfunktion sind die Aufsichtsbehörden für den Datenschutz mit weitgehenden Rechten ausgestattet. So sind nach dem HDSG alle datenverarbeitenden Stellen, dazu zählen auch Schulen, verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Dabei ist ihm insbesondere Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

Ferner haben ihm Schulleitungen bei angekündigten wie unangekündigten Kontrollbesuchen Zutritt zu allen Diensträumen zu gewähren. Aber soweit muss man es nicht kommen lassen. Guter Rat muss nicht teuer sein: „Jeder kann sich an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch datenverarbeitende Stellen (…) in seinen Rechten verletzt worden zu sein.“[1] Und was für Schülerinnen und Schüler sowie Eltern gilt, gilt auch für Lehrkräfte: „Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten wenden.“ So der § 28 Abs. 2 HDSG zur Anrufung des Hessischen Datenschutzbeauftragten. Dabei sind die Ratsuchenden auch geschützt (§ 28 Abs. 1 HDSG): „Niemand darf dafür gemaßregelt oder benachteiligt werden, dass er sich auf Grund tatsächlicher Anhaltspunkte für einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz an den Hessischen Datenschutzbeauftragten wendet.“[2]

Darüber hinaus unterliegen die Landesdatenschutzbeauftragten auch einer besonderen Schweigepflicht über die ihnen vorgetragenen Sachverhalte und Fragestellung. So lautet § 23 HDSG: „Der Hessische Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.“ Zu einer Offenlegung der Person der Ratsuchenden und Petenten gegenüber z.B. der Schulleitung oder der Schulaufsicht sind sie nicht verpflichtet.[3]

Natürlich können sich Schülerinnen und Schüler, Lehrkräfte und Eltern auch direkt an den Datenschutzbeauftragten ihrer Schule wenden (so es ihn denn überhaupt gibt). Auch der ist zur Verschwiegenheit verpflichtet (vgl. Kasten).

Hilfestellung bei der Achtung und Umsetzung des informationellen Selbstbestimmungsrechts der Schülerinnen und Schüler, Lehrkräfte und Eltern gibt es genug. Und Beratung bei den Datenschutzbeauftragten sollte nicht erst eingeholt werden, wenn „das Kind schon im Brunnen liegt“. Die Kontaktaufnahme über die Internetportale der Landesdatenschutzbeauftragten und ihre E-Mail-Adressen (siehe angehängte Liste) könnte nicht einfacher sein. Dabei ist es ja nicht unbedingt in jedem Fall erforderlich, direkten Kontakt aufzunehmen. Viele Fragen lassen sich sicher schon durch die Lektüre der über die Homepages abrufbaren schulspezifischen Informationsmaterialien beantworten. So bieten, um zwei Beispiele zu nennen, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein[4] und der Hessische Datenschutzbeauftragte[5] zahlreiche Informationen zum Schuldatenschutz auf ihrer Homepage an.

1 Siehe § 28 HDSG. Die hier am Beispiel des Hessischen Datenschutzgesetzes aufgeführten Rechte der Datenschutzbehörde bzw. der Bürgerinnen und Bürger sind in den anderen Landesdatenschutzgesetzen vergleichbar ausgestaltet.

2 Siehe dazu auch den Abschnitt „Kündigung wegen Beschwerde beim TLfD“ im 8. TB (2008/09) des Thüringer Beauftragten für Datenschutz (TLfD), Seite 64. Die Stadtverwaltung Leinefelde-Worbis hatte einem Mitarbeiter gekündigt, weil er sich direkt, ohne Einschaltung des Behördenleiters, beim Landesdatenschutzbeauftragten über seinen Dienstherrn beschwert hatte. Das Fazit des TLfD: „Ein solches Vorgehen widerspricht dem Benachteiligungsverbot von Bürgern, die bei den staatlichen Datenschützern wegen der Verletzung datenschutzrechtlicher Vorschriften um Rat und Unterstützung nachfragen oder sich über Datenschutzverstöße beschweren.“

3 So hat das Verwaltungsgericht Bremen 2010 entschieden, dass ein Landesdatenschutzbeauftragter einem Arbeitgeber nicht die Identität eines Arbeitnehmers offenbaren muss, der sich über einen Datenschutzverstoß des Arbeitgebers beschwert hatte. VG Bremen, Urteil vom 25.03.2010, Aktz. 2 K 548/09, abrufbar über www.verwaltungsgericht.bremen.de/sixcms/media.php/13/09k548-u01.pdf. Der Fall ist im 33. TB (2011) des LfD Bremen beschrieben; Landtags-Drucksache 17/1708 vom 25.03.2011, Seite 55.

4 Siehe unter https://www.datenschutzzentrum.de/schule.

5 Siehe unter www.datenschutz.hessen.de/ft-schulen.htm.

§ 5 Hessisches Datenschutzgesetz (HDSG)

Behördlicher Datenschutzbeauftragter

(1) Die datenverarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muss der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Wegen dieser Tätigkeit, bei der er frei von Weisungen ist, darf er nicht benachteiligt werden. Er ist insoweit unmittelbar der Leitung der datenverarbeitenden Stelle zu unterstellen; in Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. Der behördliche Datenschutzbeauftragte ist im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen sowie mit den zur Erfüllung seiner Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten. Die Beschäftigten der datenverarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

(2) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die datenverarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 geschützte Recht betreffen, hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die datenverarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 erforderlichen Maßnahmen zu unterstützen,
4. das nach § 6 Abs. 1 zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Abs. 2 bereitzuhalten,
5. das Ergebnis der Untersuchung nach § 7 Abs. 6 zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten und die automatisierte Datenverarbeitung nehmen. Vor einer beabsichtigten Maßnahme nach Satz 2 Nr. 1 ist er rechtzeitig umfassend zu unterrichten und anzuhören. Wird er nicht rechtzeitig an einer Maßnahme beteiligt, ist die Entscheidung über die Maßnahme auszusetzen und die Beteiligung nachzuholen.

(3) Die datenverarbeitende Stelle kann einen Beschäftigten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere datenverarbeitende Stellen können gemeinsam einen ihrer Beschäftigten zum Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird. Bestellungen von Personen, die nicht der datenverarbeitenden Stelle angehören, sind dem Hessischen Datenschutzbeauftragten mitzuteilen.

Baden-Württemberg	Der Landesbeauftragte für den Datenschutz www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen www.datenschutz-bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit www.datenschutz-hamburg.de
Hessen	Der Hessische Datenschutzbeauftragte www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern www.lfd.m-v.de
Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen www.ldi.nrw.de/
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz www.datenschutz.rlp.de
Saarland	Unabhängiges Datenschutzzentrum Saarland www.datenschutz.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte www.saechsdsb.de/
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein www.datenschutzzentrum.de
Thüringen	Thüringer Landesbeauftragter für den Datenschutz www.thueringen.de/datenschutz

Über das Internetportal „Datenschutzberichte“ der Technischen Hochschule Mittelhessen (THM) kann unter www.thm.de/zaftda/images/stories/ZAfTDa-Liste_LfD_NOEB_09122011.pdf der „Behördenkompass Datenschutzbehörden“ abgerufen werden, der auch die Anschriften, Telfonnummern etc. aller Landesdatenschutzbeauftragten enthält.

Karsten Neumann

Datenschutz in der Schule

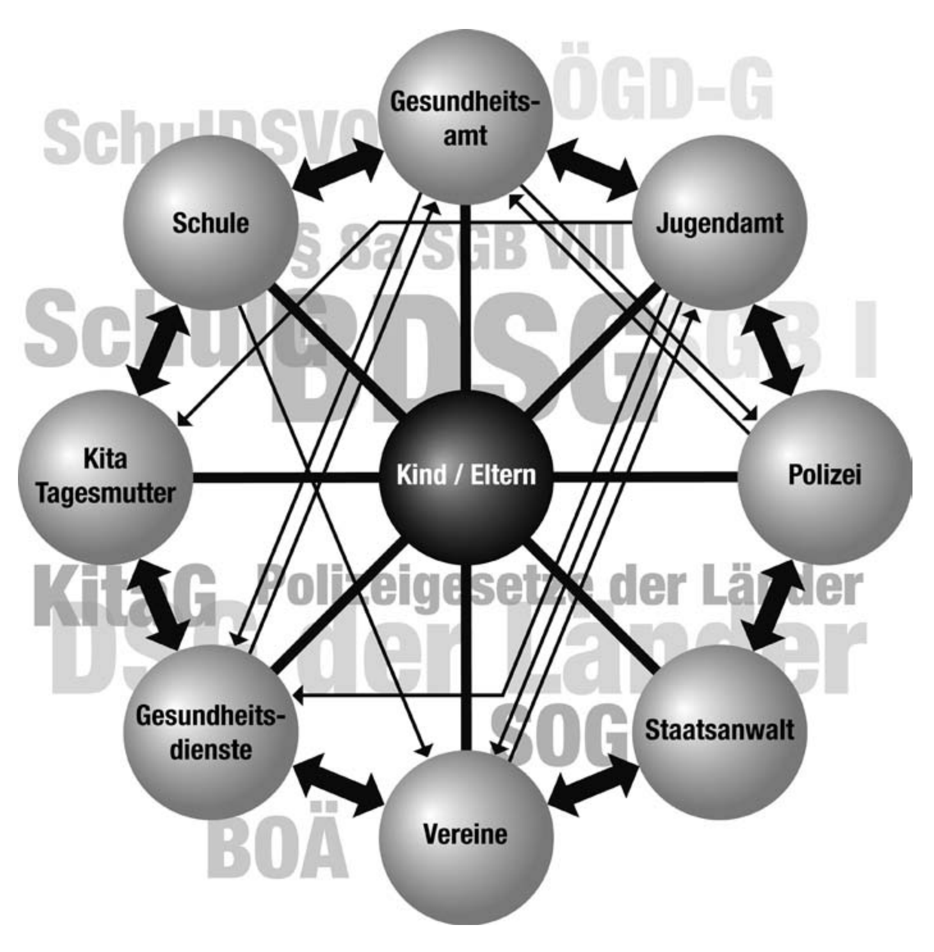
Schulrecht ist Landesrecht – ebenso wie das Datenschutzrecht in der öffentlichen Verwaltung des Landes. Insoweit dürfte es einfach sein, kohärentes Recht zu kodifizieren, das es den Akteuren einfach macht, das fachlich Erforderliche in datenschutzrechtlich zulässiger Weise zu erledigen. Dem scheint aber nicht so, wenn man die bildungspolitischen Diskussionen der Fachpolitiker und die Praxis verfolgt. Der Beschluss der Jugend- und Familienministerkonferenz „Qualitätsmerkmale und Rahmenbedingungen eines wirksamen Kinderschutzes in Deutschland", Gemeinsame Empfehlungen der Jugend- und Familienministerkonferenz und der Kommunalen Spitzenverbände vom am 31.05./01.06. 2007 war der traurige Tiefpunkt einer politisch aufgeheizten Debatte, in deren Ergebnis bis heute kein akzeptables fachspezifisches Datenschutzrecht entstanden ist.

Datenerhebung und Verarbeitung: Schule als öffentliche Stelle

Die Schule als öffentliche Stelle im Sinne des Bundesdatenschutzgesetzes unterfällt dem landesrechtlichen Regelungsvorbehalt. Soweit das Landesrecht keine Regelung trifft, ist das Bundesdatenschutzgesetz anwendbar. Die Länder haben von diesem Recht in der Regel Gebrauch gemacht. In Hessen regelt § 83 HesssSchulG ähnlich wie in fast allen Schulgesetzen als Voraussetzung für die Erhebung und Verarbeitung personenbezogener Daten, dass diese „zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist." Die Erforderlichkeit ist durch gesetzliche Bestimmungen oder Verordnungen für die schulinterne Arbeit – also die Erfüllung des Bildungs- und Erziehungsauftrags – zum Teil detailliert geregelt. Danach sind Eltern verpflichtet und die Schulträger bzw. Schulen verpflichtet, bestimmte personenbezogene Daten der Eltern und der Kinder zu erheben und zu verarbeiten. Teilweise regeln Schuldatenschutzverordnungen sehr detailliert, welche Daten zu welchen Zwecken unter welchen Bedingungen erhoben, gespeichert und verarbeitet werden dürfen. In den Bundesländern mit der Pflicht zur Bestellung von Datenschutzbeauftragten und Vertretern auch im öffentlichen Bereich sollten die personellen Voraussetzungen gegeben sein, um die Umsetzung dieser Vorgaben auch im schulischen Alltag zu überwachen. Insoweit regeln sich die Anforderungen an die Datenverarbeitung nach den allgemeinen Vorschriften für jede verantwortliche öffentliche Stelle. Dazu gehört die regelmäßige Schulung und förmliche Verpflichtung aller Lehrerinnen und Lehrer, die Erarbeitung und Durchsetzung innerbetrieblicher Regelungen für den Zugang zu Datenverarbeitungsanlagen und Dateien und die Erstellung und Bereithaltung von Verfahrensverzeichnissen, die jedermann zugänglich zu machen sind. Die Anwendbarkeit des Datenschutzrechtes beginnt jedenfalls nicht erst mit der automatisierten Verarbeitung von personenbezogenen Daten. Bereits bei Klassenbüchern handelt es sich um nicht automatisierten Dateien bzw. Akten, deren Inhalt, Zugriffsberechtigung und vor allem der Schutz gegen einen möglichen Missbrauch durch Dritte durch organisatorische und technische Maßnahmen sichergestellt werden muss. Nach diesen Maßstäben stellt die Bekanntgabe von Noten vor der gesamten Klasse eine Datenübermittlung an Dritte dar, deren Zulässigkeit sich nach der gesetzlichen Grundlage richtet. Soweit also diese Form der Datenübermittlung zur Erfüllung des Bildungs- und Erziehungsauftrages erforderlich ist, wäre sie zulässig. Diese Entscheidung ist also zuerst eine pädagogische. Anders sieht es da schon bei der Einrichtung von Internetportalen zur Information der Eltern über die Leistungsbewertung ihrer Kinder aus. Solche Internetportale erfordern ein hohes Maß an technischem Zugriffsschutz, um den Zugang nur durch Berechtigte sicherzustellen und eine vertragliche Vereinbarung mit dem Dienstleister zur Auftragsdatenverarbeitung, wie es nicht nur § 11 BDSG für Unternehmen, sondern viele Landesdatenschutzgesetze bereits für den öffentlichen Bereich vorschreiben. Bei der Verwendung von Laptops oder privater Rechentechnik durch Lehrerinnen und Lehrer sind Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer erforderlich, die an die Zulässigkeit der Nutzung dieser Technik zu dienstlichen Zwecken entsprechende Voraussetzungen für den Zugangsschutz und den Zugriffsschutz knüpfen. Eine den Stand der Technik entsprechende Maßnahme ist beim tragbaren Gerät die Festplattenverschlüsselung, die Mitnutzung durch Familienangehörige ist auszuschließen. Besondere Maßnahmen erfordert auch der Einsatz von mobilen Datenspeichern (USB-Stick, MP3-Player, elektronische Kameras), deren Nutzung aufgrund ihrer nachweislichen Gefährdung und des hohen Aufwandes für Schutzmaßnahmen generell ausgeschlossen sein sollten.

Schule als Lernort

Genauso selbstverständlich, wie elektronische Medien inzwischen im Unterricht eingesetzt werden, sollte auch die Vermittlung datenschutzrechtlicher Grundkenntnisse sein. Dazu gehört die strikte technische Trennung von Datenverarbeitungsanlagen zu Unterrichtszwecken von denen zu Verwaltungszwecken ebenso, wie die Einübung von Funktionalitäten wie Passwortgestaltung, Nutzung von Pseudonymen oder die Vorsicht bei der Verwendung personenbezogener Daten im Netz. Hier ist es auch Aufgabe der Schule, diese Themen nicht nur als technisches Wissen, sondern auch als



Die Grafik soll die Fülle der Kooperationspartner rund ums Kind darstellen und deutlich machen, dass bei jeder Informationsweitergabe jeweils zwei Rechtsgrundlagen zu berücksichtigen sind: die des „Senders“ und des „Empfängers“. Die Rechtsgrundlagen sind vielfältig: SchulG, SchulDSVO, KitaG, BDSG, DSG der Länder, SOG bzw. Polizeigesetze der Länder, ÖGD-G, SGB I, § 8a SGB VIII –der im Zentrum der Diskussion steht (Kindeswohlgefährdung), SGB X, § 203 StGB, § 138 StGB, BOÄ, …

souveräner Umgang mit den neuen Medien zu vermitteln. Dies beginnt bereits spätestens in Klassenstufe 4 bis 5 mit der Nutzung von Handys, sozialen Netzwerken und Bildern. Neben einer Fülle von Angeboten auf Landesebene zur Unterstützung des Unterrichts, der Lehrerbildung und der Elternarbeit gibt es inzwischen eine Fülle von Initiativen zum Thema Cyber-Mobbing, Internetkriminalität bis hin zu „Datenschutz geht zur Schule“ des Berufsverbandes der Datenschutzbeauftragten. Es bleibt jedoch Kernaufgabe der Schule, nicht nur den technischen Umgang mit den neuen Medien, sondern auch deren selbstbestimmte Nutzung und Schutzmöglichkeiten zu vermitteln.

Datenübermittlung: Schule als Teil des Erziehungsprozesses

Der Schwerpunkt datenschutzrechtlicher Konfliktfälle liegt jedoch regelmäßig in den Schnittstellen: Welche Datenübermittlung ist beim Übergang von der Kita in die Schule und von der Schule in die Berufsschule möglich? Was darf der Lehrer mit anderen Kollegen beraten oder dem Schulträger übermitteln? Wann darf oder muss die Lehrerin die Schulleitung oder das Jugendamt über Probleme der Schülerin informieren? Welche Informationen dürfen Lehrer und der Trainer des Sportvereines austauschen, um einen Schüler besser zu unterstützen? Wann darf die Polizei die Schule einbeziehen? Eine Fülle von Beteiligten sind gegenüber dem Kind in der einen oder anderen Weise auch datenschutzrechtlich verpflichtet: der Sportverein oder ein freier Träger der Jugendhilfe nach dem Bundesdatenschutzgesetz, das örtlich zuständige Jugendamt nach spezifischem Bundesrecht im Sozialgesetzbuch, Kinderärzte nach ihrer Berufsordnung und dem Strafgesetz, öffentlicher Gesundheitsdienst, Polizei, Schule und Berufsschule nach ihrem jeweils spezifischem Landesrecht. Im besten Fall kennt jeder der Akteure „sein“ Datenschutzrecht, was aber in der Regel nicht für eine Beurteilung der Zulässigkeit einer Datenübermittlung ausreicht. Jeder Übermittlung von Daten stellt zum einen für die „sendende“ Stelle eine besondere Datenverarbeitung dar, die nur zulässig ist, wenn und soweit ein Gesetz sie erlaubt. Für die „empfangende“ Stelle stellt sich die Datenübermittlung als Datenerhebung dar, die ebenfalls nur zulässig ist, wenn und soweit ein Gesetz sie erlaubt. Jede Datenübermittlung braucht also zwei Rechtsgrundlagen: die empfangende Stelle muss fragen dürfen, die sendende Stelle muss antworten dürfen.

Was also oft durch einzelne Akteure als mangelnde Bereitschaft zur Zusammenarbeit angesehen und kritisiert wird, kann auch eine gesetzlich angeordnete Rechtspflicht sein.

Deshalb ist der Schlüssel für eine datenschutzrechtlich zulässige Zusammenarbeit die gemeinsame Beratung aller Akteure über die jeweiligen rechtlichen Rahmenbedingungen und Befugnisse. Erst das Verständnis und der Respekt vor der jeweiligen Aufgabe des anderen kann Wege für eine akzeptale Zusammenarbeit im Konfliktfall aufzeigen. Solche „runden Tische frühe Hilfen“ oder Kooperationsvereinbarungen mit Kitas oder Kinderärzten könne zwar kein neues Recht schaffen, oft reichte aber die Kenntnis der Rahmenbedingungen bereits aus, um durch feste Verabredungen und Verfahren die erforderlichen Datenübermittlungen zu ermöglichen. Im Zweifel können die jeweiligen Landesdatenschutzbeauftragten der Bundesländer oder Datenschutzexperten beratend helfen.

Im Focus der öffentlichen und politischen Debatte steht jedoch selten die alltägliche aufopfernde Arbeit von Eltern, Pädagogen oder Sozialarbeitern, sondern tragische Fälle von Kindeswohlgefährdungen.

Kinderschutz vor Datenschutz?

Völlig zu Recht stellten die Jugend- und Familienminister gemeinsam mit den kommunalen Spitzenverbänden fest, dass „soziale Frühwarnsysteme, frühe Hilfen und Präventionsmaßnahmen so-

§ 4 – Gesetz zur Kooperation und Information im Kinderschutz (KKG):

Beratung und Übermittlung von Informationen durch Geheimnisträger bei Kindeswohlgefährdung
(1) Werden
1. Ärztinnen oder Ärzten, Hebammen oder Entbindungspflegern oder Angehörigen eines anderen Heilberufes, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologinnen oder -psychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Ehe-, Familien-, Erziehungs- oder Jugendberaterinnen oder -beratern sowie
4. Beraterinnen oder Beratern für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitgliedern oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkannten Sozialarbeiterinnen oder -arbeitern oder staatlich anerkannten Sozialpädagoginnen oder -pädagogen oder
7. Lehrerinnen oder Lehrern an öffentlichen und an staatlich anerkannten[2] privatenSchulen

in Ausübung ihrer beruflichen Tätigkeit gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder eines Jugendlichen bekannt, so sollen sie mit dem Kind oder Jugendlichen und den Personensorgeberechtigten die Situation erörtern und, soweit erforderlich, bei den Personensorgeberechtigten auf die Inanspruchnahme von Hilfen hinwirken, soweit hierdurch der wirksame Schutz des Kindes oder des Jugendlichen nicht in Frage gestellt wird.
(2) Die Personen nach Absatz 1 haben zur Einschätzung der Kindeswohlgefährdung gegenüber dem Träger der öffentlichen Jugendhilfe Anspruch auf Beratung durch eine insoweit erfahrene Fachkraft. Sie sind zu diesem Zweck befugt, dieser Person die dafür erforderlichen Daten zu übermitteln; vor einer Übermittlung der Daten sind diese zu pseudonymisieren.
(3) Scheidet eine Abwendung der Gefährdung nach Absatz 1 aus oder ist ein Vorgehen nach Absatz 1 erfolglos und halten die in Absatz 1 genannten Personen ein Tätigwerden des Jugendamtes für erforderlich, um eine Gefährdung des Wohls eines Kindes oder eines Jugendlichen abzuwenden, so sind sie befugt, das Jugendamt zu informieren; hierauf sind die Betroffenen vorab hinzuweisen, es sei denn, dass damit der wirksame Schutz des Kindes oder des Jugendlichen in Frage gestellt wird. Zu diesem Zweck sind die Personen nach Satz 1 befugt, dem Jugendamt die erforderlichen Daten mitzuteilen.

wie eine verbesserte, rechtlich abgesicherte Zusammenarbeit der Beteiligten“ notwendig sind und schlussfolgerten hieraus: „Der im Interesse des Kindeswohls erforderliche Informationsaustausch zwischen den genannten Beteiligten darf nicht an datenschutzrechtlichen Hürden scheitern, sondern ist rechtlich sicher zu stellen, insofern gilt: Kinderschutz geht vor Datenschutz.“ Selbst wenn man diese politische Formulierung auf die juristisch korrekte Formel reduziert, dass das Recht auf Leben und körperliche Unversehrtheit als Verfassungsgut alle staatliche Gewalt verpflichtet, so stimmt das unterstellte Vorrangverhältnis zum Recht auf informationelle Selbstbestimmung aus Art. 2 Absatz 1 in Verbindung mit Art. 1 Absatz 1 Grundgesetz immer noch nicht. Die Formel Kinderschutz vor Datenschutz unterstellt, dass der Schutz des informationellen Selbstbestimmungsrechtes im Konfliktfall höher bewertet werden könnte – oder wurde ? –, als das Recht auf Leben der oder des Betroffenen. Die Absurdität dieses Vergleiches offenbart sich in den gesetzgeberisch zum Glück gescheiterten Versuchen, einen solchen Vorrang zu kodifizieren.

Allein das Problem einer undurchsichtigen Fülle spezialgesetzlich normierter Datenschutzvorschriften bleibt bei den Akteuren und wurde bis heute trotz einer Fülle von Landes- und bundesgesetzlichen „Kinderschutzgesetzen“ gesetzgeberisch nicht überzeugend gelöst.

Die Rechtsgrundlage für eine Datenerhebung ohne Mitwirkung des Betroffenen in Fällen der Kindeswohlgefährdung findet sich erst in § 62, Absatz 3 Nummer 2 lit. d) SGB VIII.

(3) Ohne Mitwirkung des Betroffenen dürfen Sozialdaten nur erhoben werden, wenn … 2. ihre Erhebung beim Betroffenen nicht möglich ist oder die jeweilige Aufgabe ihrer Art nach eine Erhebung bei anderen erfordert, die Kenntnis der Daten aber erforderlich ist für…d) die Erfüllung des Schutzauftrages bei Kindeswohlgefährdung nach § 8a.

In § 4 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG)[1] soll nun geregelt werden, dass Lehrerinnen und Lehrer bei Verdachtsfällen auf Kindeswohlgefährdnung mit Kind und Erziehungsberechtigten reden sollen und die Beratung einer „insoweit erfahrenden Fachkraft“ des Jugendamtes einholen können.

Diese vorgeschlagene Neuregelung verbessert die gegenwärtig unklare rechtliche und tatsächliche Situation nicht wirklich. Die sog. „zweite Stufe“ in Absatz 3 ermächtigt zur Weitergabe personenbezogener Daten aus dem durch Berufs- und Strafrecht geschützten Vertraulichkeitsbereich. In der Begründung zum Gesetzentwurf heißt es: „Um der Praxis für die Weitergabe von Informationen an das Jugendamt größere Handlungssicherheit zu vermitteln, wird deshalb eine bundeseinheitliche Norm geschaffen. Die in Absatz 1 benannten Berufsgeheimnisträger, die von dieser Norm Gebrauch machen, handeln nicht mehr unbefugt im Sinne des § 203 Absatz 1 StGB. In diesen Fällen ist ein Rückgriff auf die allgemeinen strafrechtlichen Rechtfertigungs- und Entschuldigungsgründe entbehrlich. Außerhalb des Anwendungsbereiches der Befugnisnorm bleibt die Rechtslage unberührt.“

Im Ergebnis führt diese Regelung zu einer rechts- und fachpolitisch bedenklichen Abschaffung der ärztlichen Schweigepflicht und der daran anknüpfenden Verschwiegenheitspflichten. Diese Verschwiegenheitspflichten sind bisher eine wichtige Voraussetzung

für die Möglichkeit zur unterschwelligen Hilfe in den besonders schwierigen Bereichen. So sehr eine Klarstellung der Befugnisse zur Information des Jugendamtes in seiner helfenden Funktion zu begrüßen ist, so kritisch ist der Verlust der Vertrauensbasis für eine Hilfe durch niederschwellige Angebote zu sehen. Es droht ein Abgleiten dieser Betroffenengruppe in das Dunkelfeld für gesellschaftliche Hilfe nicht mehr erreichbarer sozialer Milieus und wäre damit zwar statistikverbessernd, aber kontraproduktiv.

In der Gesetzesbegründung greift die Bundesregierung dieses Argument selbst an – allerdings nur in Bezug auf die Schwangerschaftskonfliktberatung (Artikel 3, Nummer 1) und die begrüßenswerte Ausweitung des Rechtes auf Anonymität. Diese Argumentation gilt bei Kinderwohlgefährdungen nach der Entbindung in gleichem Maße.

Alternativ und gleich wirksam wäre es, wenn die „insoweit erfahrenen Fachkräfte“ der Jugendämter in den Schutzbereich der Schweigepflicht von Berufsgeheimnisträgern einbezogen würden und diese als eigenständig verantwortliche Stelle innerhalb der Jugendämter handeln könnten. Damit würden diese zumindest von der Amtsermittlungspflicht befreit. Dies wäre auch sachgerecht, da hierdurch eine strenge Zweckbindung der Datenverwendung sichergestellt würde und jedwede Zweckänderung (beispielsweise zur Verfolgung von Straftaten oder zur Bekämpfung von „Sozialleistungsmissbrauch“) wesentlich erschwert würde. Andererseits könnte die insoweit erfahrene Fachkraft alle Informationsressourcen der Jugendämter zur Gefährdungseinschätzung nutzen, also glaubwürdig und rechtlich abgesichert als „Sachwalter“ des betroffenen Kindes auftreten.

Mit Artikel 2 des Gesetzes soll zusätzlich das Achte Buch Sozialgesetzbuch in § 8a) geändert werden und aus dem Recht auf Beratung eine Pflicht gemacht werden. „In Vereinbarungen mit den Trägern von Einrichtungen und Diensten, die Leistungen nach diesem Buch erbringen, ist … insbesondere die Verpflichtung aufzunehmen, dass die Fachkräfte der Träger[3]… das Jugendamt informieren, falls die Gefährdung nicht anders abgewendet werden kann.“ Hiermit soll aus der strafrechtlichen Erlaubnisnorm des § 4 KKG (siehe Kasten) eine vertragliche Pflicht gemacht werden, die mithin das Ermessen der Träger der freien Jugendhilfe an die finanzielle Förderung bindet und somit „auf Null“ reduziert. Damit wird jeder Träger seine Mitarbeiterinnen und Mitarbeiter anhalten müssen, jeden Verdachtsfall „zu melden“, um der Gefahr einer Vertragsverletzung mit meist existenzvernichtenden finanziellen Folgen zu entgehen. Fraglich ist, ob die Jugendämter dieser Situation gewachsen sein werden und ob das System der frühen Hilfen, das auf Kooperationswillen der Betroffenen angewiesen ist, eine solche Meldepflicht überstehen würde. Auch wenn der Bundesrat seine Zustimmung zu dem Gesetzesvorhaben bisher verweigert hat bleibt zu befürchten, dass dies nur finanzielle, aber keine fachlichen Gründe hat.[4]

Die Lehrerinnen und Lehrer sind auf fachliche Unterstützung des Erziehungsprozesses angewiesen. Hierfür ist Informationsaustausch zwischen den verschiedenen öffentlichen und privaten Stellen dringend erforderlich. Dieser Informationsaustausch ist auf gesetzlicher Grundlage unter strikter Gewährleistung der Verschwiegenheitspflichten zu ermöglichen. Die Praxis greift heute oft in unzulässiger Weise auf Einwilligungserklärungen zurück, für deren Wirksamkeit es in der Regel an Informiertheit und Freiwilligkeit mangelt. Der Gesetzgeber bleibt gefordert, Kinderschutz und Datenschutz in einen Interessenausgleich zu bringen und nicht länger gegeneinander zu benutzen.

1 Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Stärkung eines aktiven Schutzes

2 eingefügt durch Drucksache 17/7522 – Beschlussempfehlung und Bericht

3 Klarstellung „der Träger“ eingefügt durch Drucksache 17/7522 – Beschlussempfehlung und Bericht von Kindern und Jugendlichen (Bundeskinderschutzgesetz – BKiSchG)- Drs. 17/6256 vom 22.06.2011

4 zwischenzeitlich hat der Bundestag dem Vermittlungsvorschlag zugestimmt, Drs. 17/8130 vom 14.12.2011

Manfred Weitz

Verarbeitung von Schulverwaltungsdaten auf privaten Rechnern der Lehrkräfte – die Regelungen in Hessen

1. Einleitung

Die überwiegende und ständig wachsende Zahl der Lehrkräfte an öffentlichen Schulen in Hessen nutzt den eigenen Rechner zuhause nicht nur für rein private Zwecke, sondern auch für die vielfältigen Aufgaben als Lehrkraft in der Schule. Einerseits betrifft dies den rein pädagogischen Bereich, der allerdings fast ausschließlich sachliche Unterrichtsinhalte umfasst, andererseits aber auch zahlreiche personenbezogene Daten von Schülern, Eltern und Lehrkräften, die dem Bereich der eigentlichen Schulverwaltung zuzuordnen sind, also z.B. Noten, Gutachten oder Briefe an Eltern.

Datenschutzrechtlich problematisch ist dies deshalb, weil hier vom Normalfall abgewichen wird. Dieser besteht darin, dass die personenbezogenen Daten im örtlich-räumlichen Bereich der Verwaltung verarbeitet werden, also in den Räumen der Verwaltung und dort auch im überschaubaren Gestaltungs- und Kontrollraum der Verwaltungsleitung verbleiben. Die heimische Datenverarbeitung verlässt diesen Raum und erhöht damit insbesondere mit dem Fehlen der Kontrollmöglichkeiten das Risiko fehlender IT-Sicherheitsmaßnahmen. Dies führt wiederum zu einer Gefährdungslage der betroffenen Daten, die durch angemessene Regelungen aufgefangen werden muss.

Die zuhause erfolgende Nutzung von dem Dienstherrn gehörenden oder privaten IT-Geräten für Verwaltungszwecke ist allerdings auch in anderen Verwaltungsbereichen inzwischen weit verbreitet, erinnert sei nur an den sog. Tele-Arbeitsplatz oder Richter, die zuhause Urteile vorbereiten. Auch in der Schule werden Verwaltungsprozesse mehr und mehr automatisiert und Lehrkräfte unterliegen zunehmend dem Zwang der heimischen IT-Nutzung, weil ihnen die IT in der Schule nicht ausreichend zur Verfügung steht.

2. Die Entwicklung der Regelungen in Hessen

Die bis 30. Juli 2005 geltende Fassung des früheren § 83 Abs.5 Hessisches Schulgesetz verbot die geschilderte Nutzung, ermöglichte sie allerdings nach einem entsprechenden schriftlich auf einem landesweit einheitlichen Formular gestellten Antrag nach Genehmigung durch die Schulleitung.[1] Die Details dazu waren festgelegt in der alten Fassung des § 2 der "Verordnung zur Verarbeitung personenbezogener Daten in Schulen" vom 30.11.1993.[2] Diese normativen Vorgaben wurden bis 2005 allerdings mangels Bekanntheit in der Praxis weitgehend ignoriert, wie Kontrollbesuche des Hessischen Datenschutzbeauftragten (HDSB) in Schulen ergaben. Der novellierte, ab 1. Juli 2005 geltende § 83 Abs. 5 Hessisches Schulgesetz (HSchG) enthielt das Verbot mit Erlaubnisvorbehalt allerdings nicht mehr.[3]

3. Die heutigen Regelungen

Am 1. August 2007 trat eine neue Fassung des Schulgesetzes in Kraft, die zur Nutzung des Privat-PC in § 83 Abs. 9 lediglich festlegte, dass Details, insbesondere zur IT-Sicherheit, in der erwähnten Rechtsverordnung zu regeln seien. Am 4. Februar 2009 verkündete das Hessische Kultusministerium im Amtsblatt die novellierte, nun neu titulierte „Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen"[4], die am 5. Februar 2009 in Kraft trat.[5]

4. Die wichtigsten Eckpunkte

4.1 Formale Voraussetzungen zur Zulässigkeit der heimischen PC-Nutzung:

Die oben erwähnte, frühere Genehmigung durch die Schulleitung wurde in § 3 Abs. 1 VO ersetzt durch eine schriftliche Anzeige der betroffenen Lehrkraft bei der Schulleitung über ein ebenfalls landesweit einheitlich vom Kultusministerium vorgeschriebenes Formular. Neben den geplanten Datenarten und Einsatzzwecken sind darin zu erklären: Die Verpflichtung der Lehrkraft zur Einhaltung der nach § 10 HDSG notwendigen Datensicherheitsmaßnahmen und das Einverständnis, sich der Kontrolle des Hessischen Datenschutzbeauftragten zu unterwerfen bezüglich der Einhaltung der Datensicherheitsmaßnahmen und diesem Zugang zur häuslichen Arbeitsstätte zu gewähren und die entsprechende Bereitschaft der übrigen Wohnungsinhaber.

4.2 Inhaltliche Auflagen

Die Arten der von der heimischen PC Nutzung betroffenen Daten wurden katalogartig eingegrenzt durch § 3 Abs. 2 VO und die Anlage 1, Abschnitt A6 zur VO, allerdings beschränkt auf Schülerdaten. Aufgenommen wurden in § 3 VO ebenfalls Regelungen zu Überführung der Daten in Schülerakten und Löschfristen.

§ 3 Abs. 4 VO widmet sich der Datenverarbeitung bei sog. sonderpädagogischen Gutachten, für die – wegen der meist hohen Sensibilität der Daten – erhöhte Datensicherheitsmaßnahmen verlangt werden. Ein Ausdruck des Gutachtens ist nur in der Schule erlaubt.

Eine wichtige Aussage zur rechtlichen Bewertung der heimischen IT-Nutzung für Schulverwaltungszwecke trifft § 3 Abs.5 VO: Die Schule bleibt dabei – auch für die Datensicherheit – die ver-

antwortliche datenverarbeitende Stelle. Damit wird deutlich: Die IT-Nutzung ist keine rein private Angelegenheit der Lehrkraft. Bei Verstößen gegen einschlägige Vorschriften kann nun der Schulleiter die heimische IT-Nutzung für schulische Zwecke sogar verbieten (§ 3 Abs. 6 VO).

5. Ergänzende Vorgaben des Hessischen Kultusministeriums und des Hessischen Datenschutzbeauftragten

5.1 Die Vorgaben des Hessischen Kultusministeriums

Der Verordnungsgeber war bemüht, möglichst viele notwendige und grundlegende Details zur privaten PC-Nutzung normativ festzulegen. Weitere Einzelheiten und Hilfen zu Interpretationsspielräumen, insbesondere zahlreiche Auflagen zu IT-technischen Sicherheitsfragen, fasste er – nach Abstimmung mit dem Hessischen Datenschutzbeauftragten – zusammen in seinem Erlass vom 21. August 2009.[6] So wird u.a. verlangt: Schutz vor Schadprogrammen und Bildschirmschoner. Zentral ist jedoch vor allem die Bedingung, die personenbezogenen Daten ausschließlich auf einem USB-Stick oder einer externen Festplatte zu speichern, und zwar verschlüsselt. Dies soll verhindern, dass Unbefugte sich über den illegalen Rechnerzugriff, auch über das Internet, Datenkenntnisse verschaffen können.

Mit Erlass vom 20. Mai 2010[7] stellte das HKM Zweifelsfragen klar zum Umfang der Kontrolle durch den Hessischen Datenschutzbeauftragten: Betroffen davon kann nur sein der von der Lehrkraft verwendete Rechner, nicht die sonstigen Rechner in der Wohnung.

5.2 Die Empfehlungen des Hessischen Datenschutzbeauftragten

Am 14. September 2009[8] veröffentlichte der HDSB auf seiner Homepage ein umfangreicheres Papier zu dem hier angesprochenen Problemkreis. Im Januar 2010 wurde die Broschüre „Datenschutz in Schulen“[9] veröffentlicht. Ebenfalls standen im Mittelpunkt zahlreiche Festlegungen zu den gesetzlich vorgeschriebenen IT-Sicherheitsmaßnahmen nach § 10 Abs. 2 HDSG. So werden etwa beim Einsatz eines heimischen W-LANS Verschlüsselungsmechanismen verlangt.

Wegen des erhöhten Schutzbedarfs bei sonderpädagogischen Gutachten widmete der HDSB den notwendigen Maßnahmen einen besonderen Absatz. So wird bei USB-Geräten eine bootfähige Ausführung verlangt.

6. Vollzugsprobleme

Neuregelungen wie die oben geschilderten benötigen naturgemäß etliche Zeit bei der Übernahme in der Praxis. Allerdings leidet der Vollzug im Bereich der Lehrerschaft und Schulverwaltung spezifisch daran, dass den verantwortlichen Personen oftmals das notwendige Grundwissen über die einschlägigen Datenschutzregeln fehlt, ebenfalls im Bereich der rein technischen Fragen, wie etwa bei der Frage, was eine Verschlüsselung ist. Bei Kontrollbesuchen in Schulen und Gesprächen mit Lehrkräften in Seminaren wurde dem HDSB immer wieder deutlich, dass den Schulleitungen, aber auch den schulischen Datenschutzbeauftragten eine weitgehend deutlich unterschätzte Verantwortung zukommt bei der Aufklärung der Lehrerschaft über die zahlreichen Regeln und deren Bedeutung. Augenfällig wurde und wird das Problem der Folgen fehlenden Wissens insbesondere beim Vollzug der Regelung zur formalen Anzeige der privaten PC-Nutzung bei der Schulleitung. Manche Schulleitungen haben dieses Verfahren noch nicht konsequent ins Bewusstsein genommen, andere stellen den Vollzug wegen dringenderer Aufgaben zurück. Soweit die Lehrkräfte über dieses Anzeigeverfahren aufgeklärt wurden, entwickelte sich bei vielen Lehrerschaften eine zum Teil sehr emotionale Diskussion über die Frage, ob es von der Norm her akzeptabel sein kann, dass man sich – im Rahmen der Anzeige – im eigenen Hause der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen müsse. Deshalb widmete der HDSB in seinem 39. Tätigkeitsbericht[10] dem Problemfeld ein eigenes Kapitel. So wies er auf die Regelung des § 4 HDSG hin, die eine ähnliche Risikolage reguliert wie die die private PC-Nutzung. Deutlich wurde er bei der Frage des Kontrollumfanges: „Die geäußerten Befürchtungen sind unbegründet. Es ist weder vorgesehen, die Wohnung von Lehrern zu durchsuchen noch die Rechner ihrer Familienangehörigen zu sichten.“

Die nächsten Jahre werden zeigen, welchen Akzeptanz-Grad die geschilderten Regelungen in der Praxis der Schulverwaltung erfahren werden.

1 Siehe Hajo Köppen, Datenschutz in Schulen: Das hessische Verfahren beim Einsatz von privaten PC zur Bearbeitung personenbezogener Daten von Schülerinnen und Schülern, DuD 4/1995, Seite 213.

2 Amtsblatt des Hessischen Kultusministeriums (ABl.) 2/1994, Seite 114.

3 Vgl. 34. Tätigkeitsbericht (2005) des HDSB, Seite 89, Nr. 5.6.1.

4 ABl. 3/2009, Seite 131.

5 Vgl. 38. Tätigkeitsbericht (2009) des HDSB, Seite 78, Nr. 4.5.1 und 39.Tätigkeitsbericht (2010), Seite 106, Nr. 4.5.3.

6 Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrer, Erlass vom 21. August 2009, ABl. 9/2009, Seite 726.

7 ABl. 6/2010, Seite 168.

8 Siehe unter: www.datenschutz.hessen.de/ds010.htm.

9 HDSB, Datenschutz in Schulen, abrufbar unter: www.datenschutz.hessen.de/downloads/173.pdf.

10 39.Tätigkeitsbericht (2010), Seite 106, Nr. 4.5.3.

Dr. Gabriele Heyse / Uli Vormwald

„Schule und Datenschutz in Hessen“ – Ein neues Seminar für eine neue Schule



Alle Schulen in Hessen müssen eine(n) Datenschutzbeauftragte(n) stellen. Genau für dieses Anforderungsprofil ist das Seminarkonzept „Schulen und Datenschutz in Hessen – Die Aufgaben der Datenschutzbeauftragten in der Schule“[1] von den Autoren in Kooperation mit der Goethe-Lehrerakademie der Goethe-Universität Frankfurt entwickelt worden. Das neue Konzept des dreiwöchigen E-Learning-Seminars stellt die täglichen und praxisbezogenen Aufgaben der Datenschutzbeauftragten in den Schulen in den Mittelpunkt.

Gerade in der Institution Schule ist ein verantwortungsbewusster Umgang mit den Daten, beispielsweise über Unterrichts- und Verwaltungsaufgaben, sowie über Förderungsmaßnahmen und Planungen in den Bereichen Bildung und Ausbildung gefragt. Um dies sicherzustellen, muss eine umfangreiche Aufklärung und Sensibilisierung der Eltern, SchülerInnen und Lehrkräfte erfolgen. Die Schwerpunkte des Seminars sind „Aufgaben der Datenschutzbeauftragten“, „Datenschutz im Schulalltag“, „Datenschutz und neue pädagogische Systeme“ (Nutzung des Internet in der Schule, Einsatz von Learning- Managementsystemen).

Neu akzentuiert werden die Themen Urheberrecht und Jugendmedienschutz. Gerade bei der zunehmenden Nutzung von Learning-Management-Systemen stellt sich die Frage, welche Unterrichtsmaterialien in das Intranet der Schule eingestellt werden dürfen. Mobbing im Internet ist leider kein Randthema mehr. Wir beobachten, dass dieses Thema in vielen Schulen akut ist. Daher ist es ganz wichtig und von hoher Bedeutung, dass auch Schülerinnen und Schüler mit dem Thema „personenbezogene Daten“ etwas anfangen können. Allzu leichtfertig stellen Schülerinnen und Schüler die privatesten Informationen in das Netz. Dinge, die man früher nur dem Tagebuch als geheime Verschlusssache anvertraut hat, werden heute ganz offen in den verschiedenen *social communities* ausgetauscht. Alle Aktivitäten im Internet hinterlassen Spuren, von hoher Bedeutung ist daher, dass Schülerinnen und Schüler und ganz besonders Lehrkräfte ein Bewusstsein für Datenhygiene entwickeln.

Damit dieser Transfer in die Unterrichtspraxis gelingen kann, werden Inhalte zu Themen wie personenbezogene Daten, Datensicherheit, Jugendmedienschutz, Mobbing im Internet, Datenhygiene, Datenschutz und Urheberrecht in Form von Unterrichtsmaterialien (Materialien für die Konferenzen der Lehrkräfte, Elternabende und natürlich die Schülerinnen und Schüler) aufbereitet und den Kursteilnehmern zur Verfügung gestellt. Ziel ist, dass die Kursteilnehmerinnen und Kursteilnehmer für ihre Aufgabe als Datenschutzbeauftragte vorbereitet werden.

1 Weitere Informationen, Seminar-Termine und Kursanmeldung über: www.gla.uni-frankfurt.de/veranstalt/datenschutz_schulung/index.html

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs-bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

BvD-Initiative „Datenschutz geht zur Schule“ ein Erfolgsmodell für Deutschland ?



Seit 2010 sind engagierte Datenschutzexperten aus dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. mit einem speziellen Unterrichtskonzept bundesweit ehrenamtlich an Schulen aktiv, um Schülern ab der fünften Klasse klare und einfache Verhaltensregeln für den sensiblen Umgang mit ihren persönlichen Daten im Netz näher zu bringen.

Das Internet ist für viele Schülerinnen und Schüler zu einer wichtigen Informations- und Kommunikationsplattform geworden. Per Handy und Computer sind viele Jugendliche ständig online, senden Nachrichten und stellen ungefiltert sehr persönliche Informationen oder Fotos ins Netz. Leider denken die meisten nicht darüber nach, dass diese Daten für jeden einsehbar und vor allem dauerhaft im Internet verfügbar sind. Dinge, die heute cool und top sein können, sind morgen vielleicht peinlich und bestimmen über die Möglichkeiten eines Ausbildungsplatzes mit. Das Internet ist als Leitmedium der Jugendlichen längst zum Schulhof und Jugendtreff geworden. Den meisten ist aber nicht bewusst, wer alles dauerhaft die Informationen einsehen kann und es sich dabei nicht immer nur um Freunde handelt. Die Risiken im weltweiten Netz sind so umfangreich, dass sich vor allem junge Menschen keine Vorstellungen davon machen können, was mit ihren Angaben überhaupt passieren kann.

Datenschutz als Bildungsaufgabe

Hier sieht sich auch der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. in der Verantwortung. Mit der Initiative „Datenschutz geht zur Schule“ möchte er den jungen Menschen helfen, bewusst und sensibel mit den neuen Medien umzugehen, um die Vorteile sicher nutzen zu können ohne dabei in eine der vielen möglichen Gefahren zu laufen. Aus diesem Grund wurde 2008 der Arbeitskreis „Datenschutz geht zur Schule“ gegründet, in dem – unter der Leitung von BvD-Vorstandsmitglied Thomas Floß – 15 „Datenschützer“ aus ganz Deutschland zusammen die Unterrichtsmaterialien erarbeitet, das Schulungskonzept erstellt und neue Dozenten ausgebildet haben. Seit 2010 gehen nun bundesweit ca. 30 Datenschutzexperten ehrenamtlich in die Schulen und zeigen in 90-minütigen Aufklärungsschulungen – auf Wunsch auch Lehrern und Eltern – anhand aktueller, auf die Schüler abgestimmter Themen wie Facebook, Video- und Musikdownloads, Chatrooms und Cybermobbing die Risiken und Lösungen im Umgang mit den neuen Medien auf.

Auch Datenschutz kann Spaß machen …

wenn er nicht zu trocken vermittelt wird. Genau das ist den Mitstreitern der Initiative klar. Daher wird die speziell auf die Altersstufen abgestimmte Power-Point-Präsentation auch nicht als Frontalvortrag vermittelt, sondern die Schüler aktiv mit einbezogen. Beiträge, Fragen oder eigene Erfahrungen werden besprochen und geschickt mit den klaren und verständlichen Verhaltensregeln für den sensiblen Umgang mit den persönlichen Daten verknüpft. Kleine Filme zum Thema lockern den ganzen Ablauf auf.

In der Sekundarstufe I sind es häufig diese Filme, in denen sich so mancher Schüler wiederfindet und die somit die Neugierde wecken. In der Sekundarstufe II sind eher die immer aktuellen Daten, Fakten und Beispiele von Interesse. Natürlich stoßen die Dozenten schon mal auf anfängliches Desinteresse, gemäß dem Motto „Ich weiß doch schon alles. Was will der denn jetzt von uns “ – doch das ist erfahrungsgemäß oft ein kurzfristiger Effekt, der sich schnell in volle Aufmerksamkeit wandelt, da die Schüler aktiv mit einbezogen werden und sich in vielen Themen wiedererkennen. Unsicherheiten werden deutlich, Aha-Effekte stellen sich ein und so mancher Schüler zählt mal eben die Anzahl der Stellen seines Passwortes ab, um dessen Sicherheit zu prüfen. Dass die Schüler aus dem Unterricht etwas mitnehmen, zeigen auch die vielen, im Anschluss an die Veranstaltung gestellten Fragen an den Dozenten. Um den Schülern auch nachhaltig helfen zu können, ist das Verteilen einer Checkkarte mit den sieben wichtigsten Verhaltenstipps und einer Webadresse mit wichtigen Links und Informationen zu dem Thema geplant.

Initiative „Ausgewählter Ort 2011“ im Land der Ideen

Mit dieser Initiative ist der BvD „Ausgewählter Ort 2011“ im Land der Ideen und damit Preisträger im Wettbewerb „365 Orte im Land der Ideen“, der von der Standortinitiative „Deutschland – Land der Ideen“ in Kooperation mit der Deutschen Bank unter der Schirmherrschaft des Bundespräsidenten durchgeführt wurde. Dieser Wettbewerb rückt Ideen und Projekte in den Mittelpunkt, die die Zukunft Deutschlands aktiv gestalten.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat seinen Sitz in Berlin. Seine ca. 750 Mitglieder sind als interne oder externe Datenschutzbeauftragte in mehr als 2.500 Unternehmen und Behörden bestellt.

Stellungnahme des BvD e.V. zu dem Entwurf der EU-Datenschutzverordnung

Wichtige Säule des Datenschutzes wird demontiert

Berufsverband der Datenschutzbeauftragten warnt vor Auswirkungen der Novelle

Berlin, 13.12.2011

Datenschutz in Deutschland und in Europa muss modernisiert werden – daran besteht kein Zweifel. Sowohl der deutsche Gesetzgeber, als auch die EU-Kommission haben dies erkannt und arbeiten an Entwürfen eines neuen Datenschutzes. Der nun bekannt gewordene Entwurf der neuen EU-Datenschutzverordnung beinhaltet viele neue Ansätze, die geeignet sind, dem Datenschutz in Europa ganz neue Impulse zu geben. Allerdings beinhaltet sie auch einen gewaltigen Rückschritt für den Datenschutz in Deutschland, weil sie zur Umsetzung von schlechteren Datenschutzstandards zwingt.

Da die Datenschutzrichtlinie von 1995 uneinheitlich und oft nur mit nationalen Alibi-Gesetzen umgesetzt wurde, plant die EU-Justizkommissarin Viviane Reding nun neben der inhaltlichen Änderung, die Form einer Verordnung, die dann für alle Mitgliedsstaaten verbindlich ist. Diese neue Datenschutzverordnung muss also zwingend in nationales Recht umgesetzt werden. Daher gilt es einen konsensfähigen Kompromiss zu finden, der von allen unterzeichnet werden kann. Für die deutschen Datenschutzstandards, die aus Sicht des Betroffenen als die besten der Welt gelten, bedeutet dies inhaltlich jedoch einen beispiellosen Rückschritt.

Datenschutz in Unternehmen erst ab 250 Mitarbeitern

Der größte Rückschritt ergibt sich aus der Definition eines neuen Schwellenwertes, ab dem die Bestellung eines Datenschutzbeauftragten erforderlich sein soll. Statt des bislang in Deutschland geltenden Wertes von mehr als neun Beschäftigten, die mit personenbezogenen Daten arbeiten, wird nun eine generelle Grenze ab 250 Mitarbeitern eingeführt – ganz ohne Bezug zur Datenverarbeitung.

Dieser Schwellenwert ist in mehrfacher Hinsicht geeignet, den Datenschutz in der Wirtschaft zu gefährden.

1. Datenschutz unabhängig von der Art der Datenverarbeitung

Der fehlende Bezug zur Verarbeitung personenbezogener Daten belastet Industrie- und große Handwerksunternehmen in unnötiger Weise. Unternehmen, die lediglich Mindestdaten ihrer Mitarbeiter verarbeiten, können dies oft sehr effizient mit wenigen Personen in der Verwaltung erfüllen. Einen Datenschutzbeauftragten mussten sie dafür bislang nicht bestellen. Diesen Unternehmen wird nun ein Datenschutzbeauftragter aufgezwungen, ohne das die Risiken für die Daten im Unternehmen dabei eine Rolle spielen. Dies kann nur als unnötiger Bürokratieaufbau gewertet werden.

Der BvD plädiert dafür, die Bestellung eines Datenschutzbeauftragten nicht an datenschutzirrelevante Werte, wie die Mitarbeiteranzahl zu knüpfen, sondern an Risiken wie Datenarten und Verarbeitungstechniken.

2. EU-Niederlassungen von US-Unternehmen zukünftig ohne Datenschutz

Unternehmen, die personenbezogenen Daten geschäftsmäßig verarbeiten, wie beispielsweise Callcenter, Adressmakler, IT-Outsourcer oder auch Internetdienstleister, wie Google und Facebook (Deutschland, bzw. Irland), sind zukünftig nicht mehr verpflichtet, einen Datenschutzbeauftragten zu bestellen. Diese Art von Unternehmen sind aber genau diejenigen, die bislang in Deutschland die Mehrzahl der Datenschutzskandale verursacht haben und zu deren Geschäftsfeld Datenschutz zwingend dazu gehören muss.

Die neue Bestellpflicht blendet diese risikoreichen und kritischen Verarbeitungen vollständig aus. Die neue Regelung ist daher ungeeignet, etwas zum Datenschutz beizutragen. Sie ist inhaltlich verfehlt. Im Ergebnis fehlt gerade diesen Unternehmen die wirksame Kontrolle über die Verarbeitung.

Da zahlreiche Niederlassungen von Nicht-EU Unternehmen weniger als 250 Mitarbeiter aufweisen, wird der schlechte Datenschutzstandard von US-Unternehmen oder anderer Nicht-EU-Unternehmen in deren Niederlassungen „exportiert“. Es bleibt zu hinterfragen, ob die Datenschutzverordnung Datenschutz bezwecken oder verhindern soll.

3. Auftragsdatenverarbeiter zukünftig ohne Datenschutz

Unternehmen aller Art lagern bestimmte datenschutzkritische Verarbeitungsvorgänge wie Adresserwerb, Gehaltsabrechnung, Kundenscoring, Versand, Unternehmenssicherheit (z.B. Videoüberwachung) oder IT-Betreuung aus. Mit der neuen Datenschutzverordnung würden diese externen Dienstleister bezüglich der Verarbeitungen fremder Daten von der Eigenkontrolle befreit. Schlimmer noch: große Unternehmen, die einen Datenschutzbeauftragten bestellen müssten, könnten die kritischen Verarbeitungsvorgänge auf Kleinunternehmen auslagern, die selbst keine eigenen Kontrollinstrumente aufweisen und damit der direkten Kontrolle des Datenschutzbeauftragten entziehen. Damit wird die Kontrolle in der Praxis erst recht ausgehebelt. Eine staatliche Kontrolle ist dafür gänzlich ungeeignet, da diese die realen Probleme gar nicht erfassen kann.

Der BvD plädiert daher für eine konsequente Bestellungsverpflichtung für Unternehmen, die personenbezogene Daten im Auftrag verarbeiten. Dies stellt für die Unternehmen ein Qualifikationsmerkmal zur Verarbeitung fremder Daten dar und sichert die Betroffenenrechte in diesem größten Bereich der personenbezogenen Datenverarbeitung.

4. Gesundheitsdaten sind besonders sensibel, aber ohne Schutz

Die Daten der Bereiche Religion, Gesundheit, Sexualleben, etc. verlieren den kompetenten Schutz durch den Datenschutzbeauftragten, denn auch in der Verarbeitung dieser Daten sind viele Einrichtungen kleiner als 250 Mitarbeiter. In zahlreichen Einrichtungen ist das Datenschutzverständnis schon heute gering ausgeprägt, da Kostendruck und Qualifikationsdefizite einer umfassenden Datenschutzgestaltung bereits heute entgegenstehen.

Auch für diese Einrichtungen hält der BvD eine Bestellungspflicht für den Datenschutzbeauftragten für unbedingt erforderlich, damit gerade diese Verarbeitung von besonders schützenswerten Daten nicht der direkten Datenschutzkontrolle entzogen wird.

5. Datenschutz in Unternehmen mit weniger als 250 Mitarbeitern wird abgeschafft

Der betriebliche Datenschutzbeauftragte stellt die effizienteste Säule der Datenschutzkontrolle dar. Er ist in der Regel der Treiber, der die Umsetzung der Datenschutzanforderungen überhaupt erst in die Wege leitet. Seine Nähe zu den Prozessen in den Unternehmen und seine Erfahrung im Umgang mit allen Beteiligten, machen ihn zu einer Instanz, die für die Unternehmen neben der erwünschten Datenschutzcompliance auch einen echten Wettbewerbsvorteil darstellt. Durch die Unterstützung eines erfahrenen Datenschutzbeauftragten werden überhaupt erst Datenschutzanforderungen praktikabel umgesetzt, Prozesse sicherer und oft sogar schlanker, was die Kosten senkt und das Vertrauen der Kunden regelmäßig erhöht. Fällt diese Säule für die Mehrzahl der Unternehmen weg, so werden in diesem Bereich Datenschutzanforderungen nicht mehr berücksichtigt und die Daten der Beschäftigten und die der Kunden oder Patienten nicht mehr ausreichend geschützt.

Die Erfahrung aus Deutschland hat gezeigt, dass Unternehmen, die nicht gesetzlich verpflichtet sind, einen Datenschutzbeauftragten zu bestellen, gar keine Aktivitäten im Bereich des Datenschutzes entfaltet haben. Die Anzahl der Unternehmen mit mehr als 250 Mitarbeitern dürfte bei etwa 30 % aller Unternehmen in Deutschland liegen. Das bedeutet, dass sich 70 % der Unternehmen nicht mehr mit Datenschutz befassen werden. Dabei ist es in der Praxis vollkommen bedeutungslos, dass die Verordnung auch für diese Unternehmen gilt – praktisch fällt die Kontrolle weg. Bei einer statistischen Wahrscheinlichkeit für eine Prüfung durch die Datenschutzaufsicht von ca. 38.000 Jahren, stellt die Sanktionierung durch eine Aufsichtsbehörde für die Unternehmen ein vertretbares Risiko dar.

6. Bürokratiewachstum unvermeidlich

Um die Risiken, die sich aus der Reduzierung des Datenschutzes ohne einen Datenschutzbeauftragten ergeben, im Rahmen zu halten, werden die Datenschutzaufsichtsbehörden erheblich mehr Aktivitäten entfalten müssen. Da diese schon bisher erheblich unterbesetzt sind, kann dies nur durch die Schaffung neuer Stellen in den Behörden bewältigt werden. Gesellschaftspolitisch ergibt sich damit eine Verlagerung der Arbeitsplätze aus der Wirtschaft hin zum Staat – wenn auch nicht im gleichen Maße. Auch diese Entwicklung kann wirtschaftspolitisch nicht gewünscht sein.

7. Irrglaube „Bürokratieabbau"

Die Pflicht zur Bestellung des Datenschutzbeauftragten wird fälschlicherweise oft mit der Freiheit von dieser Pflicht verglichen. Tatsächlich jedoch unterliegen Unternehmen ohne Datenschutzbeauftragten dann der staatlichen Kontrolle, weil in jedem Fall eine Kontrolle stattfinden muss. Vergleichen muss man die Situation „Bestellpflicht" daher mit der Situation „reine staatlicher Kontrolle über ein Unternehmen". In diesem Vergleich hat ein Unternehmen mit eigenem Datenschutzbeauftragten weniger Bürokratie, als ein Unternehmen unter staatlicher Aufsicht zu bewältigen. Während der betriebliche Datenschutzbeauftragte die Details einer Verarbeitung im Betrieb kennt und deshalb praktikable, schnelle und passgenaue Lösungen liefern kann, bewerten Aufsichtsbehörden in aufwändigen Verfahren, aus der Ferne und formalistisch einen Verarbeitungsvorgang. Dies ist verknüpft mit wesentlich mehr Schriftverkehr, Recherchen im Unternehmen, Ausarbeitung von Begründungen und Stellungnahmen, ohne dass dabei eine Lösung des Datenschutzproblems erfolgt. Ist gar die Genehmigung einer komplexen Verarbeitung erforderlich, läuft die neue Regelung Gefahr, die Unternehmen aufgrund von staatlicher Kontrolle auszubremsen. Solche Tendenzen zeigen sich bereits heute, wenn Unternehmen ihre Datenschutzvereinbarungen mit Nicht-EU-Partnern genehmigen lassen wollen (Code of Conduct).

Viele Europäische Staaten haben eine reine staatliche Kontrolle über die Verarbeitungsvorgänge, weisen jedoch nicht gleichwertiges Datenschutzniveau wie in Deutschland auf. Anders als deutsche Unternehmen müssen diese Unternehmen jedoch Verarbeitungen anzeigen, Meldungen durchführen und sind mit staatlicher Gängelung belastet. Deutschland hat nicht trotz, sondern wegen der Lösungen betrieblicher Datenschutzbeauftragter dieses gute Datenschutzimage.

8. Wirtschaftsfaktor „Datenschutz" gefährdet

In Deutschland sind nach groben Schätzungen des BvD über 110.000 Personen im Bereich Datenschutz tätig. Das sind interne und externe Datenschutzbeauftragte und ihre Mitarbeiter, Datenschutzberater, Unternehmen, die Softwareprodukte für diesen Bereich entwickeln, Mitarbeiter und Autoren der Verlage und inzwischen eine beachtliche Anzahl von Hochschulen, die in diesem Bereich tätig sind. Die „Teilzeitdatenschützer" sind dabei noch nicht in vollem Umfang berücksichtigt. Diese Arbeitsplätze werden in Deutschland in dem Maße verloren gehen, wie Unternehmen aus der Bestellungspflicht entlassen werden – also um etwa 70 %. Dem stehen keinerlei neue Arbeitsplätze gegenüber (mit Ausnahme der dann erforderlichen Stellen in Aufsichtsbehörden), die durch diese „Entlastung" entstehen könnten.

Aus praktischen Erwägungen und Erfahrungen plädiert der BvD schon lange für die Verbindung der Bestellungspflicht mit der Art der Datenverarbeitung im Unternehmen.

Die bisherige Koppelung des BDSG mit den „…mehr als 9 Beschäftigten, die personenbezogene Daten verarbeiten…“ war ein kleiner Schritt in diese Richtung, der nun aber komplett entfallen soll. Davor kann nur gewarnt werden. Die Auslagerung von Prozessen in den Unternehmen vor allem im Bereich der personenbezogenen Datenverarbeitung steigt. Die Unternehmen, die diese Dienstleistungen anbieten oder oft in diese Dienstleistung „herein rutschen“, haben i.d.R. keine Kenntnisse im Bereich Datenschutz und vernachlässigen den Schutz der personenbezogenen Daten ihrer Kunden regelmäßig. Erst mit der Bestellung eines Datenschutzbeauftragten wird dort die Umsetzung von Datenschutzanforderungen aufgefangen, und dies erfolgt heutzutage, weil Auftraggeber diese Bestellung einfordern. Würde man diese Eigenkontrolle abschaffen, verschlechtert dies den Datenschutz bei zahlreichen ausgelagerten Verarbeitungsvorgängen.

Besser: Qualifikation und Effektivität des Beauftragten stärken

Die Steigerung der Effektivität der Datenschutzkontrolle ist das Ziel und muss, statt über Bestellungsschwellwerte, über inhaltliche Anforderungen diskutiert werden. Ursache für auftretende Belastungen ist nicht die Institution Datenschutzbeauftragter an sich, sondern die schlechte Umsetzung. Dazu gehören mangelhafte Qualifikation von Datenschutzbeauftragten und die unzureichende Kompetenzausstattung der Datenschutzbeauftragten.

Eine Studie der Universität Oldenburg vom 08.12.2011 zum Selbst- und Fremdbild des Datenschutzbeauftragten[1] hat belegt, das Menschen den Datenschutzbeauftragten als das Überprüfungsinstrument in Unternehmen einordnen und wahrnehmen. Gleichzeitig wird aber auch eine gewisse Einflusslosigkeit des Datenschutzbeauftragten wahrgenommen. Wenn bereits das Kontrollinstrument „betrieblicher Datenschutzbeauftragter“, dass direkt im Unternehmen agiert, mit geringer Einflussmöglichkeit wahrgenommen wird, dann muss erst recht das alternative Kontrollinstrument „Aufsichtsbehörde“, dass viel weiter weg vom Unternehmensalltag agiert, als einflusslos gelten. Statt über die Abschaffung des effektiveren und von den Menschen verstandenen Kontrollinstrumentes zu sprechen, muss konsequenterweise darüber diskutiert werden, wie der Einfluss des Datenschutzbeauftragten verbessert und sein Wirken effizienter gestaltet werden kann. Hier sollte über Eingriffs- und Sanktionsmöglichkeiten nachgedacht werden.

Die Studie hat auch belegt, dass die erwartete Qualifikation an den Datenschutzbeauftragten höher ist, als die tatsächliche Ausbildung vieler Datenschutzbeauftragter. Der BvD macht seit Jahren auf die mangelhafte Ausbildung vieler so genannter „Datenschutzbeauftragter“ aufmerksam. Personen ohne ausreichende Sach- und Fachkenntnis können Prozesse behindern und fehlerhafte Bewertungen abgeben und so den Anschein erzeugen, dass Datenschutzbeauftragte an sich kostspielig und ineffektiv sind. Ursache sind jedoch mangelhafte Kompetenzen. Solange Personen mit einem Tag „Ausbildung“ diese Tätigkeit ausüben dürfen, sind solche Auswüchse weiterhin möglich.

Die Lösung der Problematik liegt jedoch in der Schaffung eines Qualifikationsniveaus für Datenschutzbeauftragte, statt in der Abschaffung des Instruments Datenschutzbeauftragter. An ihn sollten genauere Anforderungen formuliert und eine verbesserte Ausbildung etabliert werden.

Das Modell des betrieblichen Datenschutzbeauftragten hat sich deshalb so bewährt, weil der betriebliche Datenschutzbeauftragte nicht nur die Verarbeitungsvorgänge x-fach genauer kennt als die Aufsichtsbehörde, sondern auch, weil er die Risiken einer Verarbeitung wesentlich treffsicherer identifizieren kann: mit höchst individuellen Lösungen im Datenschutz.

Es ist deshalb notwendig, dass auf der Grundlage der genannten Studienergebnisse die Rolle des Datenschutzbeauftragten weiter ausgestattet und gestärkt werden.

Fazit

Eine wirtschaftsfreundliche Novelle? Selbst das nicht. Es ist zu erwarten, dass die Verarbeitung von Daten schwerer wird: Jeder Bürger in der EU ist auch ein Betroffener. Erfahrungsgemäß endet die Bereitschaft jede Datenverarbeitung zu akzeptieren, sobald man selbst oder die eigenen Kinder betroffen sind. Dies gilt sogar für Bürger der USA.

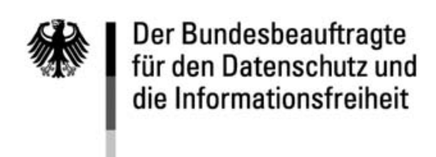
Aus den hier erläuterten genannten Gründen kann dieser vorgelegte Entwurf der EU-Datenschutz Verordnung nur als ein bitterer Rückschritt angesehen werden. Der BvD plädiert daher für die Anpassung der genannten Punkte, bevor die Umwandlung dieser Verordnung in geltendes Recht erfolgt.

1 Beim BvD erhältlich.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. in Berlin ist der älteste und größte Berufsverband für Datenschutzbeauftragte in Deutschland. Die überwiegend internen sowie die externen Datenschutzbeauftragten, die im BvD organisiert sind, betreuen mehrere tausend Unternehmen in Deutschland und sind so für hunderttausende Betroffene als Ansprechpartner im Bereich Datenschutz tätig. Die Erfahrungen und das Know-how dieser Datenschutzexperten bündelt der BvD in Fachgruppen. In Zusammenarbeit mit anderen Verbänden und Datenschutzaufsichtsbehörden hat der BvD das Berufliche Leitbild des Datenschutzbeauftragten entwickelt, dass heute als Standardwerk und die Grundlage für die Tätigkeit des Datenschutzbeauftragten gilt.

Der BvD ist Träger des Preises „365 Orte im Land der Ideen“, den er für sein ehrenamtliches Projekt „Datenschutz geht zur Schule“ (https://bvdnet.de/365orte.html) erhalten hat. Dies ist das zurzeit größte Projekt in Deutschland, in dem Experten direkt in den Schulen Jugendliche, Lehrer und Eltern zum sicheren Umgang mit Internet und Datenschutz unterrichten. Ohne die Unterstützung der zahlreichen betrieblichen Datenschutzbeauftragten im BvD wäre dieses Projekt nicht mehr möglich.

Sie erreichen den Autor unter thomas.spaeing@bvdnet.de.



Internationale Datenschutzkonferenz setzt starkes Signal für mehr Datenschutz im Internet

Pressemitteilung 36/2011
Bonn/Berlin, 4. November 2011

Unter dem Motto „Datenschutz im globalen Zeitalter“ tagte die 33. Internationale Datenschutzkonferenz vom 2. bis 3. November in Mexiko-Stadt, an der Datenschutzaufsichtsbehörden aus aller Welt teilnahmen, darunter auch – erstmalig als Vollmitglied – die US-amerikanische Federal Trade Commission. Die Konferenz fasste einen Beschluss zur Gewährleistung des Datenschutzes bei der anstehenden Umstellung auf den neuen Internetstandard IPv6. Dazu erklärt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar:

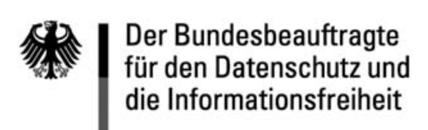
„Die Internationale Datenschutzkonferenz sendet mit ihrem einstimmigen Beschluss eine starke Botschaft an die Anbieter von Internetdiensten und an die Hersteller von Hard- und Software. Angesichts der zunehmenden Registrierung des Nutzungsverhaltens und der Profilbildung müssen bei der Umstellung auf den neuen Standard die Möglichkeiten für einen datenschutzgerechten Einsatz von IPv6 gewährleistet werden. Es ist nicht hinzunehmen, dass etwa die Hersteller von Smartphone-Software überwiegend die weltweite eindeutige Hardware-Kennung der Geräte als Bestandteil der IP-Adresse verwenden. Sie nehmen damit billigend in Kauf, dass das Verhalten der Nutzer individuell zugeordnet werden kann.“

Das neue Internetprotokoll Version 6 (IPv6) könnte zu einem Autokennzeichen für jeden Internetnutzer werden. Wer sich aber ständig mit demselben Kennzeichen im Netz bewegt, kann sehr leicht und dauerhaft verfolgt und wiedererkannt werden. Um die Wiedererkennung und Nachverfolgung im Netz weltweit zu minimieren, hat die Internationale Datenschutzkonferenz nun grenzüberschreitende Anforderungen an die Umstellung auf das neue Internetprotokoll benannt.

Wie diese Anforderungen auf nationaler Ebene von den Betreibern umgesetzt werden können, soll auch Gegenstand eines Symposiums sein, das der Bundesbeauftragte in Kooperation mit dem Museum für Kommunikation am 22. November 2011 durchführt. Weitere Informationen hierzu stellt Ihnen die Pressestelle in Kürze zur Verfügung.

Alle Ergebnisse der 33. Internationalen Datenschutzkonferenz, darunter eine Entschließung zum datenschutzkonformen Handeln nach Naturkatastrophen, finden Sie unter www.datenschutz.bund.de

Verantwortlich: Peter Schaar
Redaktion: Juliane Heinrich
Pressestelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
telefonisch 030 18 77 99 916 oder
0172 2503700 oder per E-Mail pressestelle@bfdi.bund.de.



Smart Meter – Smarter Datenschutz in intelligenten Stromnetzen

Pressemitteilung 39/2011
Bonn/Berlin, 06.12.2011

Anlässlich der aktuellen Diskussion über die technische Gestaltung von intelligenten Stromzählern – Smart Meter – legt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am Tag des Sechsten Nationalen IT-Gipfels ein Positionspapier (s. Anlage) zu den Datenschutzanforderungen an Smart Meter vor.

Peter Schaar: „Wer smart und erfolgreich sein will, kommt ohne Datenschutz nicht aus. Dies gilt auch für Smart Meter. Die modernen Zähler sollen den Stromverbrauch, nicht jedoch den Stromverbraucher, transparent machen. Auch hier gilt, die besonderen Erfordernisse des Datenschutzes bereits zu einem frühen Zeitpunkt zu berücksichtigen und den Datenschutz von vorneherein in die Gesamtkonzeption (Privacy by Design) einzubeziehen, anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand beheben zu müssen. Diese Vorgehensweise führt auch zu einer höheren Akzeptanz bei den Verbrauchern.“

Erfahrungen in anderen Ländern haben gezeigt, dass ein angemessener Datenschutz wesentlich zu einer erfolgreichen Einführung von Smart Meter beiträgt. Viele Aktivitäten in Beruf, Familie und Freizeit spiegeln sich auch in einem nach Energieeinsatz und Nutzungszeit spezifizierten Verbrauchsprofil wider. Da eine sehr detaillierte Verbrauchserfassung technisch möglich ist, können aussagekräftige Nutzungsprofile erstellt werden. Dies birgt ein hohes Ausforschungspotential in Bezug auf die Lebensgewohnheiten der Betroffenen. Auf den Punkt genau und in Echtzeit wird die einzelne Aktivität erkennbar. Über den Tag ergibt sich auf diese Weise ein Ablaufprotokoll, das wesentliche Informationen für ein Persönlichkeitsprofil enthält.

Smart Meter und Datenschutz

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) begrüßt eine nachhaltige und effiziente Energieversorgung. Jedoch darf diese nicht zum gläsernen Energieverbraucher führen. Anlässlich der aktuellen Diskussion über die technische Gestaltung von Smart Meter, abgebildet im Schutzprofil des Bundesamtes für Sicherheit in der Informationstechnik, weist der BfDI nachdrücklich auf folgende Punkte hin:

Datenschutz als Erfolgskriterium für Akzeptanz

Der Erfolg von Smart Meter ist unmittelbar abhängig von einer hohen Akzeptanz der Verbraucher. Die Gewährleistung eines angemessenen Datenschutzes stellt dabei das wesentliche Erfolgskriterium dar. Dies belegen Meldungen aus den Niederlanden und Kanada beispielhaft: Hier hatte die Nichtbeachtung von Datenschutz- und Datensicherheitsaspekten in einer frühen Phase zu einer massiven Ablehnung der neuen Stromzähler bei der Bevölkerung geführt.

Lokale Datenhaltung im Smart Meter

Daten, die von Smart Metern erhoben werden, sollen nur dann den Haushalt verlassen, wenn dies erforderlich ist. Ansätze, bei denen Verbrauchsdaten hoch aufgelöst von einer zentralen Stelle gespeichert, aufbereitet und weitergeleitet werden, und bei denen erst in der zentralen Stelle geprüft wird, ob die Daten zur Verarbeitung überhaupt erforderlich sind, lehnt der BfDI ab.

Derartige zentrale Datensammlungen widersprechen den Grundsätzen der Datensparsamkeit, Datenvermeidung, Erforderlichkeit und Zweckbindung.

Lokale Umsetzung variabler Tarife im Smart Meter

Zur Umsetzung variabler Tarife sollen Smart Meter wirklich intelligent sein und die notwendigen Berechnungen zur Verbrauchsermittlung in Tarifzonen selbst durchführen. Nur so kann verhindert werden, dass der Verbraucher detaillierte Verbrauchsdaten zur Nutzung neuer Tarife preisgeben muss. Davon zu unterscheiden sind die Ermittlung der Rechnungsbeträge, die Rechnungserstellung sowie der Rechnungsversand, die auch außerhalb des Smart Meter erfolgen können.

Lokale Verbrauchsvisualisierung beim Verbraucher

Mit einer lokalen Schnittstelle von Smart Meter zum Verbraucher soll sich jeder Verbraucher ein Bild über seinen Energieverbrauch machen, ohne dass sensible Verbrauchsdaten im Sekundentakt an Dritte weitergeleitet werden müssen. Nur so hat der Verbraucher die Möglichkeit, sich an den Energieeffizienzmaßnahmen zu beteiligen, ohne datenschutzrechtliche Kollateralschäden in Kauf nehmen zu müssen.

Zum Hintergrund

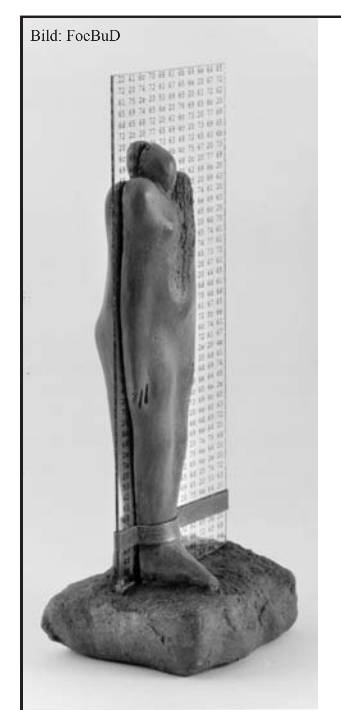
Der BfDI hat sich bereits frühzeitig für bereichsspezifische gesetzliche Vorgaben eingesetzt, die die Erhebung, Verarbeitung und Nutzung der durch Smart Meter erhobenen Daten regeln. Hierbei fordert er:

- Strikte Zweckbindung der anfallenden Daten
- Nutzung personenbezogener Daten nur soweit erforderlich
- Grundsatz der Datensparsamkeit
- Transparente Information über die Datenverarbeitungstatbestände
- Datenhoheit beim Verbraucher (z.B. bei Fernmessen und Fernwartung)
- Verbindliche Standards für den technischen Datenschutz sowie die IT-Sicherheit
- Wahlfreiheit für datenschutzfreundliche Lösungen (Verbrauchsvisualisierung, Umsetzung variabler Tarife, lokale Datenhaltung beim Verbraucher)

Der Detaillierungsgrad der Daten birgt datenschutzrechtliche Risiken. Die Möglichkeit von differenzierten und engmaschigen Nutzungs- und Verhaltensprofilen in den Haushalten schafft ein großes Ausforschungspotenzial. Ein gläserner Energiekunde bzw. -nutzer muss vermieden werden. Datenschutzrechtlich problematisch stellen sich auch die neuen Rollen bei Energienutzung, Lieferung und Abrechnung dar. Neue Akteure bedeuten, dass mehr personenbezogene Daten als bisher verarbeitet und genutzt werden. Damit steigt das Fehler- und Missbrauchsrisiko.

BigBrotherAwards 2012

Bild: FoeBuD



Die »Oscars für Überwachung« (Le Monde) werden am Freitag, 13. April 2012 um 18 Uhr im Rahmen einer großen Gala in der Hechelei der Ravensberger Spinnerei in Bielefeld verliehen. Eintrittskarten erhalten Sie im Vorverkauf über den FoeBuD-Webshop. Die Gala wird live als Video-Stream gezeigt.

Die DVD will diese Aktion finanziell unterstützen. Dazu wird Ihre Hilfe gebraucht.

Es ist ganz einfach: Überweisen Sie Ihren Betrag auf das Konto 59 4 59 5 02 bei der Postbank Köln (BLZ 370 100 50) bis spätestens zum 13. April 2012. Geben Sie als Verwendungszweck „BigBrotherAwards 2012“ an. Wir garantieren, dass alle Spenden vollständig und ohne Abzug dieser Veranstaltung zugute kommen. Verspätete Zweckspenden werden natürlich auch noch ordnungsgemäß weitergegeben.

Helfen Sie mit!

BIG BROTHER AWARDS.de

Thilo Weichert

Dopingbekämpfung und Persönlichkeitsschutz

Zugleich Besprechung von Johannes Niewalda, „Dopingkontrollen im Konflikt mit allgemeinem Persönlichkeitsschutz und Datenschutz“, Duncker&Humblot, Berlin 2011, 732 S., ISBN 978-3-428-13349-9 (u.a.), und Peter Wedde, Rechtsgutachten zum Thema „Datenschutzrechtliche Bewertung der Melde- und Kontrollpflichten im Rahmen von Anti-Dopingmaßnahmen, die die von SP.IN vertretenen Athleten betreffen“, 5. September 2011, http://www.spinbb.net/uploads/media/Wedde_-_Gutachten_fu__r_SP.IN_per_5.9.2011.pdf

I. Einführung

Doping und Datenschutz – ein vor kurzem noch unbearbeitetes Feld – entwickelt sich zu einem beachteten Thema in der Rechtswissenschaft und in der Praxis. Beiträge hierzu liefern die Doktorarbeit des Vorstandsmitglieds der Nationalen Anti-Doping-Agentur (NADA) Lars Mortsiefer „Datenschutz im Anti-Doping-Kampf“ (siehe dazu die Besprechung von Weichert in DuD 2011, 702 ff.) und die Untersuchung des Landesbeauftragten für Datenschutz Rheinland-Pfalz (LfD Rh.Pf.) und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH) mit dem Titel „Datenschutz und Dopingbekämpfung“ (https://www.datenschutzzentrum.de/allgemein/20110726-positionspapier-dopingbekaempfung.html). Eine weitere zum Thema erarbeitete aktuelle Doktorarbeit von Johannes Niewalda sowie ein von Peter Wedde für die „spieler.initiative basketball – SP.IN“ erstelltes Rechtsgutachten sollen hier vorgestellt werden.

Sämtliche dieser Arbeiten wurden weitgehend unbeeinflusst voneinander erstellt, was zur Folge hat, dass die Ausarbeitungen noch nicht in einem kontroversen Diskurs zusammengeführt wurden. Dass sie hierfür bestens geeignet sind, dafür stehen die vier völlig voneinander abweichenden Untersuchungsansätze und deren Ergebnisse: Die beiden Dissertationen kommen im Wesentlichen zum Ergebnis, dass das bestehende Doping-Bekämpfungssystem in Einzelpunkten überarbeitet werden muss, strukturell aber rechtlich nicht zu beanstanden sei. Die Untersuchungen der Datenschutzaufsichtsbehörden und von Wedde verwerfen dagegen genau diese Gesamtstruktur. Während Mortsiefer bei seiner Arbeit offensichtlich durch seine Tätigkeit bei der NADA interessengeleitet ist, verfolgt Niewalda ein akademisches Interesse. Das ULD SH und der LfD Rh.Pf. wiederum haben die Aufsichtsbrille auf, während Wedde das Thema aus der Arbeitnehmerperspektive betrachtet.

Das Thema stößt nicht nur auf diese partikularen Interessen, sondern ist inzwischen auch in der öffentlichen Debatte angekommen. Dies ist zum einen dem Umstand geschuldet, dass hier für ein höchst publikumswirksames, ja spektakuläres Ziel, die Dopingbekämpfung im Leistungssport – auch aus rechtlicher Sicht – nicht minder spektakuläre Maßnahmen ergriffen werden: der Aufbau eines globalen Systems mit einer fast totalitären Persönlichkeitsbeeinträchtigung der betroffenen Sportlerinnen und Sportler. Zugleich steht das Thema im doppeltem Sinn für den technolgischen Fortschritt, einmal biotechnologisch – für die menschliche Leistungssteigerung – zum anderen technisch – durch ein informationstechnisch großkalibriges, leider nicht besonders ausgeklügeltes Kontroll- und Überwachungssystem. Insofern ist der Diskurs über Doping und Persönlichkeitsrechte zugleich stellvertretend für die Debatte um industriellen und technischen Fortschritt und die Wahrung der Menschlichkeit, Grundrechte und demokratische Strukturen.

II. Niewalda

Niewaldas bei Prof. Klaus Vieweg erstellte Promotion ist in mehrfacher Hinsicht schwer verdaulich: Auf 745 Seiten fühlt sich jemand, der klare und nachvollziehbare Lösungen zu realen Problemen sucht, schnell verloren. Es ist aber nicht nur der schiere Umfang dieses Werkes, sondern auch die juristische Herangehensweise, die einem Datenschützer, und nicht nur diesem, die Arbeit im Hals stecken lässt: Niewalda bearbeitet in seiner Arbeit das zivilrechtliche allgemeine Persönlichkeitsrecht und den Datenschutz, als hätten diese beiden Dinge juristisch erst einmal nichts direkt miteinander zu tun. Dann aber legt er an die Datenschutzfragen bei der Dopingbekämpfung einen lockeren zivilrechtlichen Maßstab an, der weder in der Rechtsprechung des Bundesverfassungsgerichtes noch in der Praxis der Aufsichtsbehörden zu finden ist und der allenfalls den Applaus der sportlichen und politischen Funktionäre finden kann.

Das entwickelte Legitimationsmuster ist es wert, dargestellt zu werden: Der grundrechtliche Ausgangspunkt ist die in Art. 9 GG geschützte „Vereinsautonomie“ im Sport, aus der Niewalda eine Dopingbekämpfungsbefugnis ableitet. Ohne die Dopingbekämpfung seien die Sportvereine in ihrer Existenz und ihrer selbstdefinierten Identität gefährdet. Zwar wird ausführlich das allgemeine Persönlichkeitsrecht und der Datenschutz dargestellt; doch werden diese voll unter das Primat des Vereinszwecks Dopingverbot gestellt. Dass dabei die Grundrechte der Sportlerinnen und Sportler betroffen sind, wird nicht ausgeblendet, aber über die Fiktion wirksamer zivilrechtlicher Absprachen und Einwilligungen kleingearbeitet. Aus dem Vereins- und unausgesprochenen Vertragszweck „dopingfreie Sportausübung“ wird eine übergreifende datenschutzverweigernde Zweckbestimmung der im Anti-Doping-System tatsächlich stattfindenden Datenverarbeitung gemacht.

Aus der Erforderlichkeit des Ziels folgt die Erforderlichkeit der Maßnahmen und auch deren Angemessenheit, wobei Niewalda keine Scham kennt, weder vor dem Urinieren unter Sichtkontrolle, noch vor urologischen und gynäkologischen Untersuchungen, ja selbst nicht vor genetischen Tests und Langzeitprobenprofilen. Niewalda kombiniert dabei in seltsamer und in rechtlich unzulässiger Weise die Freiwilligkeit der von den Athletinnen und Athleten erpressten Einwilligungen mit der Interessenabwägung bzw. einer Verhältnismäßigkeitsprüfung: Weil eine Maßnahme verhältnismäßig ist, sei sie freiwillig. Auch das Verfahren der Aufenthaltskontrollen, also die Verarbeitung der „Whereabouts", wird entsprechend gerechfertigt.

Überraschend ist dann, dass nach einer grundrechtlichen Beliebigkeit in den großen Fragen bei praktischen Umsetzungsfragen plötzlich eine kritische Sichtweise vertreten wird. So betont der Autor immer wieder die Wichtigkeit der Pseudonymisierung, etwa bei den Urinproben oder beim Meldesystem. Welcher persönlichkeitsrechtliche Mehrwert dadurch entstehen sollte, erschließt sich aber nicht so richtig. Die Probensicherung und -versendung sei „verbesserungsfähig und insoweit unwirksam". Die Regeln des NADA-Codes zur Blutabnahme müssten verständlicher gefasst und konkretisiert werden. Geradezu skurril sind die Erörterungen über die Erforderlichkeit der elektronischen Verarbeitung von Aufenthaltsdaten angesichts der alternativen Möglichkeit der Verarbeitung „in Papierform". Es werden ausführliche Abwägungen vorgenommen, wobei der Autor eine klare Aussage zur Rechtmäßigkeit immer wieder schuldig bleibt, wenn er dann meint, eine bestimmte Maßnahme im Rahmen der Dopingbekämpfung könne zulässig sein, wenn sie im Einzelfall verhältnismäßig wäre. Dabei blendet er aus, dass alle Einzelfälle vom Gesamtsystem geprägt werden.

Der Autor hat Fakten über Fakten zusammengetragen und präsentiert diese eloquent und unterhaltsam. Das Buch hat zweifellos Stärken: Dies sind zum einen die Materialfülle, dann aber auch das Ansprechen von vielen bisher wenig erörterten Themen wie z. B. die Relevanz von Sponsorenverträgen oder die Anwendbarkeit der Regeln zum automatisierten Abrufverfahren auf das international von der WADA betriebene Meldesystem ADAMS. Dogmatisch richtig wird die Problematik der Verarbeitung von Gesundheitsdaten durchdekliniert, die nicht durch den § 28 Abs. 6-9 BDSG abgedeckt ist. Welche Folgen das für die realen Dopingkontrollergebnisse hat, bei der es fast ausschließlich um Gesundheitsdaten geht, wird der geneigten LeserIn aber vorenthalten.

III. Wedde

Das Gutachten von Wedde ist in fast jeder Hinsicht ein Gegenstück zu der Arbeit von Niewalda: Kurz und knapp wird auf 154 Seiten in der Expertise für die Basketballer-Vereinigung SP.IN trocken und juristische zielgerichtet der NADA-Code anhand der geltenden Datenschutz- und Arbeitsrechtsregeln abgeklopft. Dabei fällt der Code in praktisch jeder Hinsicht durch:

Zwar können bei der Dopingbekämpfung berechtigte Interessen nach § 28 Abs. 1 Nr. 2 BDSG geltend gemacht werden, doch greifen die geregelten und praktizierten Maßnahmen unverhältnismäßig in die schutzwürdigen Betroffeneninteressen ein. Die Anforderungen des AGB-Rechtes (§§ 305 ff. BGB) werden ebenso missachtet wie die an wirksame datenschutzrechtliche Einwilligungserklärungen. Eine Freiwilligkeit kann bei dem als alternativlos vorgesehenen Verfahren nicht angenommen werden. Auch das Arbeitsrecht verbietet eine derart invasive Datenerhebung und -verarbeitung. Dieses vernichtende Ergebnis gilt sowohl für das Melde- wie für das Testverfahren.

IV. Was nun tun?

Die Argumente liegen alle auf dem Tisch. Sie zeugen von einem hohen Diskussionsbedarf, da sie noch allzu weit auseinanderliegen. Dabei befinden sich alle Beteiligten in einem Dilemma, wenn sie Doping wirksam bekämpfen und Persönlichkeitsrechte wirksam wahren wollen, was niemandem der Beteiligten in letzter Konsequenz abgesprochen werden kann. Das weltweite Anti-Dopingsystem lässt sich nur schwer national einhegen. Weltweit werden sowohl die Dopingbekämpfung wie der Datenschutz mit äußerst unterschiedlichem Maße gemessen. Der gewählte Weg über das Sportrecht als spezielles Zivilrecht lässt den Sportlerinnen und Sportler mit ihrem Anspruch auf Datenschutz und Privatsphäre alleine. Alleine gelassen werden sie bisher auch von der Politik und den Verbänden. Die Verbände meinen ebenso wenig verantwortlich zu sein wie der Staat. Tatsächlich sollten sowohl die sportlichen wie die politischen Funktionäre aber ein Interesse nicht nur an einem sauberen, sondern auch an einem grundrechtsverträglichen Sport haben. Kürzlich fand im Deutschen Bundestag im Sportausschuss eine erste Anhörung statt, was auf eine Sensibilisierung zumindest der gewählten Politikerinnen und Politiker schließen lässt.

Der zu gehende Weg sollte klar sein: Zunächst müssen sich sowohl auf Verbands- wie auf politischer Ebene die Verantwortlichen zur Nachjustierung der nationalen Verfahren bekennen. Hier ist eine ganze Menge möglich: verstärkte Beteiligung der Sportlerinitiativen, bessere Auskunfts- und Beschwerderechte, abgestufte, an der Verhältnismäßigkeit orientierte Verfahrensgestaltung, technische bessere, transparentere und sichere Ausgestaltung des Verfahrens.

Stoßen die nationalen Reformbemühungen an die Grenzen der globalen WADA-Vorgaben, so muss der Konflikt auch in die WADA und auf das internationale Parkett gebracht und dort ausgetragen werden. Die Sport- und Politikverantwortlichen müssen insofern noch hinreichend motiviert werden, sich für die Grundrechte ihrer Sportlerinnen und Sportler auf internationaler Ebene einzusetzen. Bis dahin ist es noch ein weiter Weg. Letztlich ist der Umgang mit dem Persönlichkeitsschutz bei Dopingkontrollen ein Lackmustest dafür, welche Rolle Grundrechtsschutz und demokratische Verfahren in einem globalen (Sport-) Markt und in einer hochtechnisierten Welt spielen können und sollen.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Behördenübergreifende Rechtsextremistendatei geplant

Polizei und Geheimdienste in Deutschland sollen nach dem Willen von Bundesinnenminister Hans-Peter Friedrich (CSU) schon bald Infos über militante Rechtsextreme und Kontaktleute in einer Datei einspeisen. Gemäß einem eilig nach dem Auffliegen von mehreren Neonazimorden und gewaltigen Ermittlungspannen durch den Tod der Rechtsextremisten Uwe Mundlos und Uwe Böhnhardt im November 2011 zusammengeschusterten Gesetzentwurf sollen die jeweiligen Kriminalämter, Verfassungsschutzbehörden und der Militärgeheimdienst MAD dort nicht nur Informationen über „Verdächtige, Beschuldigte, Täter oder Mittäter einer politisch rechts motivierten Gewalttat mit extremistischem Hintergrund" einspeisen, sondern auch Informationen über Rechtsextreme, die zur Gewalt aufrufen oder „Gewalt als Mittel zur Durchsetzung politischer Belange bejahen". Gemäß dem Entwurf sollen auch Kontaktleute solcher gewalttätigen oder gewaltbefürwortenden Neonazis in der beim Bundeskriminalamt (BKA) an dessen Zweitsitz Meckenheim angesiedelten Datei gespeichert werden. Danach dürfte es wenige Rechtsextreme in Deutschland geben, die am Ende nicht in dieser Datei landen können, da die rund 25.000 Mitglieder zählende Szene deutschlandweit über die Landesgrenzen eng vernetzt ist und die Grenzen zur Gewaltbereitschaft fließend sind. Zusätzlich zu grundlegenden Angaben über Namen und Aliasnamen, die Funktion in einer rechtsextremen Organisation, Adressen oder besondere körperliche Merkmale sollen zu den Personen in dem Anti-Nazi-Register auch Angaben über Waffenbesitz, Kenntnisse im Umgang mit Sprengstoff oder ihre vermutete Gefährlichkeit eingespeist werden können („erweiterte Grunddaten") sowie Telefonnummern, Bankverbindungen und E-Mail-Adressen von gewalttätigen oder gewaltbefürwortenden Rechtsextremen. Behörden, die Informationen abrufen wollen, erhalten nicht automatisch auf alle zu einer Person gespeicherten Daten Zugriff, sondern je nach Zweck und Dringlichkeit.

Das Vorbild für das gemeinsame Neonazi-Register von Polizeibehörden und Geheimdiensten ist die Anti-Terror-Datei, die als Reaktion auf die Anschläge vom 11. September 2001 entstanden ist. Sie war nach langen Diskussionen im Jahr 2007 eingerichtet worden – und zwar gegen die Stimmen von Grünen, Linkspartei und FDP im Bundestag. 2009 hatte die FDP der Union im Koalitionsvertrag das Versprechen abgerungen, „die bestehenden Sicherheitsdateien" zu evaluieren. Die Anti-Terror-Datei und dessen Projektdateien sind gemäß dem zugrunde liegenden Gesetz, das derzeit vom Bundesverfassungsgericht auf seine Vereinbarkeit mit dem Grundgesetz geprüft wird, ausschließlich auf die Ermittlung gegen Islamisten ausgerichtet, ohne dass dies so explizit ins Gesetz geschrieben wurde. Deshalb meint die CDU/CSU nun ein neues Gesetz zu benötigen. In der FDP sind nicht alle glücklich über das Tempo, mit dem Innenminister Friedrich als Reaktion auf die Mordserie des „Nationalsozialistischen Untergrunds" (NSU) eine ähnliche Datei gegen gefährliche Rechtsextremisten vorantreibt. Der parlamentarische Geschäftsführer der FDP-Bundestagsfraktion, Christian Ahrendt, meinte: „Jetzt muss erst mal aufgeklärt werden, welche Fehler die Sicherheitsbehörden gemacht haben, sodass Neonazis über Jahre hinweg mordend durchs Land ziehen konnten. Erst wenn man sich hier ein vollständiges Bild macht, kann die Politik handeln." Ähnlich sehen das Datenschützer, die vor den generellen Risiken von Zentraldateien mit vielen zugriffsberechtigten Sicherheitsbehörden warnen.

Rundum ablehnen wollen die Liberalen die Anti-Nazi-Datei wegen der schwierigen öffentlichen Vermittelbarkeit nicht. Justizministerin Sabine Leutheusser-Schnarrenberger (FDP) zeigte sich offen gegenüber einer zusammengeführten Datei, wenn dadurch die Informationen über Neonazis, Kameradschaften und gewalttätige Rechtsextreme verbessert werden könnten. Sie wolle sich aber nun erst mal „intensiv" mit dem Entwurf von Innenminister Friedrich befassen (SZ 16.11.2011, 1; Höll SZ 29.11.2011, 1; Schmidt www.taz.de 30.11.2011).

Bund

2010 vier große Strafverfolgungs-Lauschangriffe

Gerichte haben im Jahr 2010 in vier Fällen den umstrittenen großen Lauschangriff zur Strafverfolgung angeordnet. Der am 14.09.2011 dem Bundeskabinett vorgelegte Jahresbericht führt die Abhöraktionen in Privaträumen auf. Im Jahr 2009 gab es neun Fälle; 2008 waren es sieben. Anlässe waren in Baden-Württemberg, Hamburg und Niedersachsen im Jahr 2010 schwere Straftaten wie die Bildung krimineller oder terroristischer Vereinigungen, das Einschleusen mit Todesfolge sowie gewerbs- und bandenmäßiges Einschleusen. Dabei wurden eine Privatunterkunft und drei „sonstige Wohnungen" verwanzt. Die einzelnen Aktionen dauerten den Angaben zufolge zwischen einem Tag und 70 Tagen, wobei in einem Fall Übersetzungskosten in Höhe von 9.500 und in einem anderen in Höhe von 10.000 Euro anfielen. Restliche Aufwendungen werden mit Summen

zwischen 500 und 2.000 Euro beziffert. Als relevant für das Anlassverfahren erwiesen sich die Lauschangriffe dem Report nach in drei Fällen, Bedeutung für weitere Strafverfolgungen erlangten sie nicht.

Der große Lauschangriff wurde 1998 von der schwarz-gelben Bundesregierung eingeführt. 2004 hatte das Bundesverfassungsgericht die Maßnahme zwar grundsätzlich gebilligt, aber Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung gefordert. Aus Protest gegen den großen Lauschangriff war Justizministerin Sabine Leutheusser-Schnarrenberger (FDP), die damals schon einmal Ressortchefin war, 1996 zurückgetreten. 2005 gaben Richter in sieben Verfahren einem Gesuch nach einer akustischen Wohnraumüberwachung statt, 2006 in drei, 2007 in zehn Ermittlungsfällen. Davor lag die Zahl der genehmigten Wanzeneinsätze jeweils bei rund 30 pro Jahr (SZ 15.09.2011, 6; Krempl www.heise.de 29.09.2011).

Bund

Ca. 80.000 Widersprüche gegen Bing Street Side

Während Google wegen seines Dienstes Street View in den Jahren 2008/2009 nicht aus den Schlagzeilen herauskam, erlangten die seit Mai 2011 stattfindenden Kamerafahrten für den Konkurrenten Microsoft Bing weniger Aufmerksamkeit. Laut Microsoft gab es bis Ende September 2011 etwa 80.000 Vorabwidersprüche gegen Maps Streetside von MieterInnen und HausbesitzerInnen, die nicht wollen, dass ihre Hausfassade im Internet zu sehen ist. Gegen den vergleichbaren Dienst Google Street View, der im November 2010 in Bezug auf 20 deutsche Städte startete, waren 244.287 Widersprüche eingegangen. Der Suchmaschinenbetreiber sagte zu, in diesen Fällen die Bilder zu verpixeln und die Rohdaten unwiderruflich zu löschen. Gemäß Google-Sprecherin Lena Wagner ist die Zahl der Zugriffe auf den Kartendienst Google Maps in den Gebieten, wo Street View integriert worden ist, in einem Jahr um 25% angestiegen.

Der für den Microsoft-Dienst zuständige Präsident des bayerischen Landesamtes für Datenschutzaufsicht Thomas Kranig meinte, seine Behörde habe ab August 2011 mit einem Anstrum gerechnet, tatsächlich seien nur wenig Anfragen eingegangen, es herrsche „fast tote Hose“: „Offenbar haben sich die Gemüter rund um dieses Thema beruhigt.“ Microsoft meint, man habe davon profitiert, dass sich die Menschen bei Google Street View ein Bild davon machen konnten, wie ein solcher Dienst funktioniert, und deshalb jetzt eine eigene „sachliche Risiko-Nutzen-Abwägung“ vornehmen können. Tatsächlich wollte Microsoft zunächst, anders als letztlich Google, keine Vorabwidersprüche zulassen. Eine Selbstregulierung des Branchenverbandes BITKOM zu Internet-Panoramadiensten sieht einen solchen Vorabwiderspruch nicht vor. Auf massiven Druck der Datenschutzbehörden hatte sich dann Microsoft aber auf die selben Kriterien eingelassen, die zuvor mit Google verabredet worden waren.

Google erklärte inzwischen, seinen Dienst Street View in Deutschland nicht weiterführen zu wollen. Vorläufig würden keine weiteren Städte im Netz präsentiert. Zwar waren 2011 wieder Kameraautos auf der Straße. Diese sollten aber ausschließlich dafür sorgen, den Kartendienst Maps auf dem neuesten Stand zu halten. Anderswo macht Google immer mehr Informationen zugänglich. In sechs Parks von Madrid bis Tokio lässt sich inzwischen spazieren gehen; die Bilder wurden mit Kamerafahrrädern eingefangen. Inzwischen bietet Google, von Kalifornien ausgehend, einen weiteren Service: Restaurants und Geschäfte können innerhalb ihrer Räume in einem Rundgang präsentiert werden. So sollen sich mögliche KundInnen eine Vorstellung vom Ambiente und vom Sortiment machen können (Der Spiegel 35/2011, 72; www.n24.de 23.05.2011; Kuhn SZ 19./20.11.2011, 14).

Bund

CDU-Mitgliederdaten geklaut

Wie erst am 26.08.2011 bekannt wurde, ist das Mitgliedernetz der CDU im August 2009 Opfer eines Hackerangriffs geworden. Die Partei informierte betroffene Mitglieder per E-Mail. Es habe sich herausgestellt, dass die Einbrecher beim Angriff Zugriff auf Mitgliederdaten hatten und diese dann am 12.08.2011 im Internet veröffentlichten. Dabei handele es sich um den Nachnamen, eine interne Kennnummer und die E-Mail-Adresse. Wie viele Datensätze betroffen sind, wie der Angriff erfolgte und warum die CDU ihre Mitglieder erst nach zwei Jahren über die Kompromittierung der Daten informierte, blieb unklar. Die CDU hatte im Jahr 2009 rund 530.000 Mitglieder, die reale Zahl der im Mitgliedernetz angemeldeten BenutzerInnen dürfte aber aufgrund der Altersstruktur der Partei deutlich geringer sein. Eine Mitarbeiterin der technisch verantwortlichen CDU-Wirtschaftstochter Union Betriebs-GmbH bestätigte den Hackerangriff. Ein CDU-Sprecher erläuterte, der Hackerangriff 2009 sei zwar registriert worden, zum damaligen Zeitpunkt habe aber kein Datenverlust festgestellt werden können. Erst vor wenigen Tagen sei man von einem Mitglied darauf hingewiesen worden, dass in der Hackerszene eine CDU-Mitgliederliste kursiere und diskutiert werde. Betroffen seien 5.800 Mitglieder, die nun per E-Mail über den Datenverlust informiert wurden; bislang konnte noch kein Missbrauch der Daten festgestellt werden. Die ursächliche Sicherheitslücke sei bereits 2009 geschlossen worden (www.heise.de 26.08.2011).

Bund

Mehr Transparenz bei Ärztehonoraren

Die Regierungskoalition will für mehr Transparenz bei Ärztehonoraren sorgen. Die GesundheitsexpertInnen der Union und der FDP haben im November 2011 beschlossen, dass künftig die KassenpatientInnen auf der Homepage ihrer gesetzlichen Krankenkasse einsehen können sollen, wie viel ihre ÄrztIn für Behandlungen und Verordnungen abgerechnet hat. Schon jetzt kann einE PatientIn nach dem Arztbesuch eine Quittung verlangen. Das passiert aber so gut wie nie. Zum einen interessiert es viele nicht, weil die Kasse ohnehin alles abrechnet. Viele scheuen sich aber

auch, weil sie fürchten, die ÄrztIn könne dies als Zeichen des Misstrauens interpretieren. Oft sind zudem die aufgeführten Posten schwer zu verstehen, was die Quittung nicht unbedingt populärer macht. Schließlich ist die Quittung nur begrenzt aussagekräftig, weil sie nicht anzeigt, was eine ÄrztIn tatsächlich erhält, da sie beim Verfassen nicht weiß, ob es noch Abschläge auf die Summe gibt und wie hoch diese sein werden.

Die Versicherten sollen künftig bei allen 153 gesetzlichen Krankenkassen kontrollieren können, ob nur das in Rechnung gestellt wurde, was tatsächlich geleistet wurde. Einbezogen sein soll auch die ambulante Behandlung von Ärzten und Zahnärzten. Die Kasse darf aber gemäß dem Gesetzesvorschlag weiterhin keinen Zugriff auf diese Arztkosten haben, weil ihr aus Datenschutzgründen verboten ist, die Gesamtausgaben für einen individuellen Versicherten zu berechnen. CSU-Gesundheitspolitiker Johannes Singhammer erläutert: „Das ist ein entscheidender Schritt zu mehr Transparenz“ (Der Spiegel 46/2011, 77; SZ 15.11.2011, 5; siehe auch unten NRW/Schleswig-Holstein).

Hamburg

Datei über auffällige Jugendliche eingerichtet

Die Hamburger Polizei führt ohne ausreichende Rechtsgrundlage eine zentrale Datei mit einem Ampelsystem über zunächst 288 auffällige Jugendliche ein. Schulen, Jugendhilfe, Jugendbewährungshilfe, Polizei und Staatsanwaltschaft sollen wöchentlich berichten, etwa ob die Jugendlichen die Schule geschwänzt haben. Ist das der Fall, werden die Betroffenen im Ampel-System von Grün über Gelb nach Rot eingestuft. Steht die Ampel für einen Jugendlichen auf Rot, lädt die Polizei zur „Fallkonferenz“.

Die Ampel-Datei im Hamburg wurde für junge Menschen unter 21 Jahren eingeführt. Wöchentlich werden 54 Kriterien von fünf Behörden überprüft. Einige Beispiele: Schule: Gute Noten in Kernfächern: grün. Ab fünf Tage Fehlzeit: gelb. Gewaltmeldung der Schule: rot. Jugendhilfe: Absprachen werde eingehalten: grün. Klient gilt als nicht erreichbar: rot. Jugendgerichtshilfe: Tritt eine persönliche Krisensituation ein, gelb, hält diese länger an oder kommt kein Kontakt zustande: rot. Polizei: Opfer häuslicher Gewalt: gelb.

Dieses „Obachtsverfahren“ sei, so Sozialsenator Detlef Scheele (SPD) bei der Vorstellung Ende Oktober 2011, datenschutzrechtlich geprüft. Die eine Behörde könne nicht die Daten einer anderen sehen. Diese „Draufsicht“ habe nur die Koordinierungsstelle bei der Polizei. Die besagten „Fallkonferenzen“, die 2008 in Hamburg und 2009 in Bremen eingeführt wurden, sind jedoch allgemein in der Kritik. Dort sitzen Polizei, Sozialarbeit, Schule, Bewährungshilfe und manchmal die Ausländerbehörde zusammen, um über einen jungen Menschen zu sprechen. Doch Sozialarbeiter sind zur Verschwiegenheit verpflichtet, machen sich sogar strafbar, wenn sie Geheimnisse ihrer KlientInnen bekannt geben. Das hat den Zweck, ein Vertrauensverhältnis zu ermöglichen. Ähnliches gilt für Jugendbewährungshelfer. Die Polizei, die die Runden leitet, unterliegt demgegenüber dem „Legalitätsprinzip“: Sie müsste eigentlich jede Straftat verfolgen, von der sie erfährt.

Wenn Professionen mit verschiedenen Befugnissen zusammensitzen, kann das aus Sicht von Datenschützern schief gehen. Ein Ausweg ist eine „Einwilligungserklärung“ der Jugendlichen, wie es sie in Bremen gibt. Doch Bremens Datenschutzbeauftragte Imke Sommer sagt, eigentlich sei dies „keine einwilligungsfähige Situation“. Eine Zustimmung müsste permanent widerrufbar sein. Da der Jugendliche nicht mit am Tisch sitzt, sei dies „ein Problem“. Die Bremer Rechtswissenschaftlerin Andrea Kliemann hat sich 2010 in einem Fachaufsatz mit den „Fallkonferenzen“ in Bremen und Hamburg beschäftigt und empfiehlt „dringend“ deren Abschaffung. Das Konzept führe für Sozialarbeiter zu einer „schwer erträglichen Situation“. Nehmen sie teil, laufen sie Gefahr, sich strafbar zu machen. Tun sie es nicht, bräuchten sie ein hohes Maß an Rechtskenntnis und Selbstsicherheit. Das bestätigen auch Jugendamtsmitarbeiter in einem Evaluationsbericht der Universität Hamburg. Die Atmosphäre bei „Fallkonferenzen“ sei so, dass nur die wenigsten es schafften, persönliche Daten zu verweigern.

Das neue Ampel-System ist für Kliemann „skandalös“. Damit würden Jugendliche, die in Vergangenheit auffällig waren, durch eine „praktisch grenzenlose“ Datensammlung überwacht. Es sei nicht nachvollziehbar, worin die rechtliche Übermittlungsbefugnis für Schule und Jugendhilfe bestünde. Dies zerstöre Vertrauen und führe dazu, dass Betroffene noch schwerer erreichbar seien. Schulen, Jugendgerichtshilfe und Jugendbewährungshilfe würden „zu Informanten der polizeilichen Strafverfolgung“, befürchtet die Linkspartei-Abgeordnete Christiane Schneider. Besser wären dezentrale „Fallkonferenzen“ mit den Jugendlichen und ohne Aufsicht durch die Polizei. Die Polizei handelt ohne rechtliche Grundlage. Sie brauche für solch eine Datensammlung eine „Errichtungsanordnung“, im Zuge derer alle fachspezifischen Datenschutzfragen geklärt werden müssten.

Das bestätigt auch der Hamburgische Datenschutzbeauftragte Johannes Caspar. Fehle die Anordnung, führe das „zu einem rechtswidrigen Verfahren“. Dies könne aber nachgeholt werden. Caspar hält das jetzige Verfahren für bedenklich. Jugendämter dürften die wenigsten Daten weitergeben, die Polizei habe dagegen den größten Spielraum. Wenn bei ihr nun die meisten Erkenntnisse über die Jugendlichen aus den Jugendämtern zusammenliefen, entspräche dies „nicht der gesetzlichen Ausgangssituation“. Er schlug vor, dass die Sozialbehörde Trägerin des Verfahrens wird. Deren Sprecher Oliver Klessmann bestätigt, dass es Gespräche mit dem Datenschutz gab und „Optionen geprüft“ würden. Bis dahin könne erst mal alles so weiterlaufen (Kutter www.taz.de 20.11.2011).

Hamburg

Betrüger täuschen mit Telefonnummer des Datenschutzbeauftragten

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) informierte, dass Anrufe vom „Datenschutz Hamburg“, der

„Datenschutzzentrale Hamburg“ oder „Aktion Datenschutz“, bei denen um Vorkasse für eine Beratungsleistung oder einen Gutschein gebeten wird, betrügerisch sind und nichts mit der Dienststelle des HmbBfDI zu tun haben. In der letzten Zeit hätten sich dort Beschwerden über solche unseriösen Anrufe gehäuft. Entweder wird um Vorauszahlung für Datenschutzleistungen gebeten oder der Angerufene soll dem Postboten 79,95 Euro mitgeben, um dafür einen Gutschein über 700 Euro zu erhalten. Eine besondere Qualität haben diese betrügerischen Anrufe dadurch, dass auf dem Display des Angerufenen eine Telefonnummer erscheint, die der des Hamburgischen Datenschutzbeauftragten täuschend ähnlich ist, und dass der Name einer Mitarbeiterin des HmbBfDI benutzt wird. Der HmbBfDI Johannes Caspar wies darauf hin, dass er nie telefonisch um die Zahlung eines Geldbetrages bitten würde. Angesichts der vermehrten Betrugsversuche hat sich seine Dienststelle an die Hamburger Staatsanwaltschaft gewandt, um dem rufschädigenden Missbrauch ihrer Kontaktdaten ein Ende zu setzen. Betroffene BürgerInnen sollten sich ebenfalls an die Polizei oder Staatsanwaltschaft wenden (PM HmbBfDI 22.08.2011).

Niedersachsen

Seltsame Presseakkreditierungen durch Polizei

Der Deutsche Journalisten Verband (DJV) kritisierte die Akkreditierungspraxis der Polizei vor dem Castortransport Ende November 2011 nach Gorleben und äußerte die Befürchtung, dass JournalistInnen vom Bundeskriminalamt (BKA) und vom Verfassungsschutz durchleuchtet würden, wenn sie bei der Polizei einen Akkreditierungsantrag stellen. Die niedersächsische Polizei empfahl allen JournalistInnen, die vom Atommülltransport berichten wollen, neben regulären Presseausweisen eine vorherige Akkreditierung bei der zuständigen Polizeidirektion Lüneburg. Dort prüfe man, ob ausreichend Arbeitsproben vorlägen und der Antragsteller tatsächlich Journalist sei, so eine Sprecherin der Lüneburger Polizeidirektion. Nach erfolgreicher Prüfung stellte die Polizei einen Akkreditierungsausweis aus. Der Ausweis solle „Einsatzbeamten vor Ort“ ermöglichen, MedienvertreterInnen auf einen Blick und ohne längere Prüfung zu erkennen. Zwar akzeptiere man im Einsatzgebiet des Castors auch reguläre Presseausweise, der von der Polizei ausgestellte Ausweis ermögliche jedoch volle Mobilität, ohne längere Wartezeiten an den Kontrollpunkten.

Der DJV kritisiert dieses Verfahren. Er vergebe, nach strengen Kriterien, zusammen mit weiteren fünf Verbänden einen Presseausweis, der sich in Deutschland als anerkanntes Dokument durchgesetzt hat, so DJV-Sprecher Hendrik Zörner. Jedes Jahr schicke man der Polizei ein Musterexemplar. „Beamte im Einsatz könnten die Ausweise der Journalisten mit einem unserer Musterexemplare vergleichen.“ Die Polizei Lüneburg trat den Befürchtungen des DJV entgegen. Man werde die JournalistInnen, die einen Akkreditierungsantrag stellen, nicht durchleuchten. „Wir geben die jeweiligen Namen lediglich bei Google ein“, so eine Sprecherin der Polizeidirektion Lüneburg (Dachsel wwww.taz.de 09.11.2011).

Nordrhein-Westfalen

Deutsche Post nutzt Lügendetektoren im Ausland

Der Personalvorstand des in Bonn sitzenden Konzerns Deutsche Post, Walter Scheurle, räumte in einem Brief an die Gewerkschafts-Dachorganisation UNI Global Union den Einsatz von Lügendetektoren-Tests bei Mitarbeitenden im Ausland ein: „Lügendetektoren werden in Ländern verwendet, in denen der Einsatz legal ist, und nur bei außergewöhnlichen Umständen“. Als Beispiel nennt Scheurle Kolumbien, wo es Konflikte mit Milizen und Drogenkartellen gibt. Der Einsatz von Lügendetektoren sei in einer internationalen Richtlinie geregelt und begrenzt. Die internationale UNI Global Union, zu der auch die deutsche Dienstleistungsgewerkschaft Verdi gehört, hatte zuvor protestiert: „Die Beschäftigten der Deutschen Post DHL in Panama, Costa Rica, Kolumbien und Südafrika werden gezwungen, sich Lügendetektortests zu unterziehen.“ Konkret soll es um den Fall eines Mitarbeiters des zur Post gehörenden Logistikunternehmens DHL in Kolumbien gegangen sein. Dieser habe wegen 22 fehlender USB-Sticks den Test machen müssen. Ein Postsprecher bestätigte, die Post AG sei wegen des Detektoreinsatzes schon länger mit den Gewerkschaften vor Ort im Gespräch. Schon früher gab es – auch wegen der Lügendetektoren – von Gewerkschaftsseite Kritik an den Arbeitsbedingungen von DHL im Ausland. DHL beschäftigt nach eigenen Angaben 275.000 Menschen in mehr als 220 Ländern (SZ 19.09.2011, 20).

Nordrhein-Westfalen

Exakte Geo- und Adressdaten für jedes Gebäude in Deutschland

Die Deutsche Post Direkt und die Bezirksregierung Köln haben einen Kooperationsvertrag unterzeichnet, in dem die Verschneidung der postalischen Daten mit dem bundesweiten Referenzdatenbestand der amtlichen Hauskoordinaten der deutschen Vermessungsverwaltung, die bei der Bezirksregierung Köln gebündelt werden, vereinbart wird. Das Ergebnis ist die größte georeferenzierte Gebäudedatenbank Deutschlands. Die hausgenaue Lokalisierung wird mittlerweile z. B. im behördlichen Umfeld, für Navigations- und Zustelldienste, beim Netzbetrieb und für die Standortplanung sowie für die Zielgruppen-Findung werbungtreibender Unternehmen genutzt, wobei der Genauigkeit und Zuverlässigkeit der Daten eine zunehmende Bedeutung zukommen. Mit Hilfe der amtlichen Hauskoordinaten wird die Position von mehr als 20 Millionen Gebäuden in Deutschland präzise bestimmt und mit den korrekten postalischen Angaben verknüpft. Anders als durch Interpolation berechnete Daten zeichnen sich die von den Vermessungsverwaltungen erho-

benen Hauskoordinaten durch hohe geometrische Lagegenauigkeit aus. Quellen der Hauskoordinaten sind die Liegenschaftskataster der Länder, in denen alle Flurstücke und Gebäude in Deutschland geführt werden. Die postalischen Daten stammen aus der Gebäudedatenbank der Deutschen Post, die alle bundesweit zustellrelevanten Gebäude umfasst.

Aufgrund der Kooperation bietet die Deutsche Post Direkt ab sofort zwei etablierte Produkte im Adressmanagement zusätzlich mit hausgenauen Geodaten an: Datafactory Geocode enthält Geokoordinaten auf Postleitzahl-, Straßen- und Gebäudeebene sowie die geocodierten Flächen der Postleitzahlgebiete in Deutschland. Werbungtreibende können die Geodaten in ihre eigenen Applikationen integrieren, die Adressen ihrer Kundendatenbanken prüfen und in digitalen Karten raumbezogen darstellen. Damit werden beispielsweise Verkaufsgebiete und Marktpotenziale visualisiert, Standorte geplant und der Vertrieb gesteuert. Mit Hilfe von Addressfactory sollen Werbungtreibende die Qualität und Zustellbarkeit ihrer KundInnendaten verbessern können. Die Adressaktualisierung erfolgt auf Basis der Postreferenz-Datei von der Deutschen Post Direkt, die mehr als 190 Millionen aktuelle und ehemalige Privatadressen umfasst. Durch die Anreicherung der exakten Koordinaten auf Gebäudeebene können Kundenadressen jetzt präziser für die Vertriebsoptimierung, Routen- oder Standortplanung qualifiziert werden.

Mit dem aktuellen Update der amtlichen Hauskoordinaten ist erstmals ein bundesweites Produkt des Liegenschaftskatasters der Länder verfügbar, das zur bedarfsgerechten Aufbereitung um postalische Informationen aus originärer Quelle ergänzt wurde. Die hausgenauen amtlichen Geodaten bieten Nutzenden neben präzisen Koordinaten und detaillierten Informationen zu Verwaltungsschlüsseln nun auch Zugriff auf postalische Inhalte der Deutschen Post Direkt, wie Postleitzahl, Ortsname und Ortsteil. Damit werden hausgenaue Analysen und Prozesse weiter vereinfacht und „bringen maximale Sicherheit in strategische Unternehmensentscheidungen" (www.vdv-online.de 30.09.2011; PM Deutsche Post Direkt 22.09.2011).

NRW/Schleswig-Holstein

AOK-Patientenquittung für mehr Transparenz

Für mehr Transparenz im Gesundheitswesen soll die AOK-PatientenQuittung in Westfalen-Lippe (Nordrhein-Westfalen) und Schleswig-Holstein sorgen. Als erste große gesetzliche Krankenkasse in Deutschland bietet die AOK NordWest ihren 2,8 Millionen Versicherten diesen besonderen Service. Ein Testlauf von einigen Wochen hatte zuvor gezeigt, dass der Dienst gut angenommen wird. Frank Simolka, AOK-Regionaldirektor: „Patienten wollen wissen, was ihre Gesundheit kostet. Diesem Wunsch kommen wir gern nach. Mit der AOK-PatientenQuittung verschaffen wir unseren Kunden einen umfassenden Überblick über nahezu alle Leistungen, die über ihre Krankenversichertenkarte abgerechnet wurden.". KundInnen der AOK NordWest können auf Wunsch seit September 2011 kostenlos nahezu alle Leistungen einsehen, die über ihre Krankenversichertenkarte abgerechnet wurden. Nach etwa zwei Monaten Laufzeit haben sich nach Angaben der Kasse schon 15.000 Versicherte registrieren lassen. Der Sprecher der AOK NordWest Jens Kuschel hofft, „dass das Schule macht". Der Service soll von allen regionalen Verbänden der AOK eingeführt werden.

Die AOK-PatientenQuittung zeigt zum Beispiel auf, welche Behandlungen beim Arzt oder Zahnarzt in Anspruch genommen und abgerechnet, welche Zuzahlungen erfolgt sind oder welche Medikamente zu welchem Preis und in welcher Apotheke in Rechnung gestellt wurden. Beim Angebot der AOK NordWest fehlen die Ausgaben für ambulante Behandlungen bei einem Arzt oder Zahnarzt. Die Online-Abfrage ist für AOK-KundInnen jederzeit möglich. Der Service wurde datenschutzrechtlich überprüft und soll den höchsten Sicherheitsanforderungen genügen. Wolfgang Zöller, CSU-Bundestagsabgeordneter und Patientenbeauftragter der Bundesregierung, meint: „Hier wird ein großer Schritt hin zu mehr Transparenz für die Patienten gemacht" (www.dtoday.de 14.09.2011; Christiansen, Genoux Kieler Nachrichten 03.09.2011, 1, 2, 19; SZ 15.11.2011, 5; s. o. Bund).

Rheinland-Pfalz

Frauenarzt fotografierte heimlich Patientinnen

Mehrere Jahre lang soll ein Frauenarzt seine Patientinnen während der Behandlung fotografiert und Intimbilder erstellt haben. Polizei und Staatsanwaltschaft gehen von mehr als 3.000 betroffenen Frauen aus. Mindestens 35.000 Fotos wurden bei einer Durchsuchung Ende August 2011 in der Praxis sichergestellt, so der Leiter der Staatsanwaltschaft Frankenthal, Lothar Liebig. Nach Bekanntwerden der Vorwürfe stellten mehr als 700 Patientinnen Strafantrag. Der 56jährige Arzt hatte sich noch nicht zum Tatvorwurf geäußert; er schloss seine Praxis freiwillig. Nach den bisherigen Erkenntnissen hat der Arzt die Bilder nicht weiterverbreitet (SZ 08.09.2011, 10; SZ 22.11.2011, 10).

Schleswig-Holstein

Arzt beobachtete heimlich PatientInnen per Video

Ein niedergelassener Arzt aus dem Raum Lübeck hat seine PatientInnen über Jahre hinweg heimlich in seiner Praxis mit drei Videokameras überwacht. Der Mediziner, der unter anderem Darmspiegelungen vornahm, hatte zwei Kameras in Behandlungsräumen hinter Leitz-Ordner-Imitaten versteckt installiert; eine weitere befand sich im Anmeldebereich. Nachdem ein Patient dies entdeckt und Strafanzeige erstattet hatte, bekam der Arzt im September 2010 zwecks Durchsuchung der Praxisräume Besuch von der Staatsanwaltschaft und dem Unabhängigen Landeszentrum für Datenschutz (ULD). Dabei wurden die drei Kameras gefunden, die über eine drahtlose WLAN-Verbindung mit Computern verbunden waren. Auf

den Festplatten der Computer konnten jedoch keine Aufnahmen sichergestellt werden. Der Arzt verteidigte sich mit dem Hinweis, die entsprechenden Räume würden auch als Aufwachräume genutzt. Er wolle seine PatientInnen mit den Kameras nach einer Narkose beobachten können. Die Mediziner gestand ein, die Überwachung schon seit über 8 Jahren zu betreiben, ohne dass seine PatientInnen hierüber informiert worden wären.

Die Staatsanwaltschaft stellt das Strafverfahren ein und gab es an das ULD als Ordnungswidrigkeitenbehörde weiter. Das ULD verhängte ein Bußgeld von 500 Euro. Der Leiter des ULD, Thilo Weichert, meinte, wegen der Dauer des Videoeinsatzes hätte der Fall nicht mehr als Bagatelle eingestuft werden können. Auf den Einspruch des Arztes hin stellte das Amtsgericht auch das Bußgeldverfahren ein, was Weichert verärgerte: „Wenn von Gerichten derart mit solchen Fällen umgegangen wird, ist fragwürdig, ob von uns verhängte Bußgelder überhaupt noch abschreckend wirken.“ Die Ärztekammer Schleswig-Holstein wollte „wegen der Schweigepflicht“ zum konkreten Fall keine Stellung beziehen. Kammersprecherin Kirsten Lorenz meinte: „Videogestützte Therapien, z. B. in einer orthopädischen Praxis, sind unbedenklich, wenn das Einverständnis des Patienten eingeholt wurde und sie für die Dokumentation des Therapieerfolges relevant ist.“ Wichtig sei außerdem, dass das Videomaterial vereinbarungsgemäß verwendet wird. Der betreffende Arzt hat inzwischen seine Praxis aufgegeben – aus Altersgründen (Tönnemann, Lübecker Nachrichten 09./10.10.2011, 7).

Datenschutznachrichten aus dem Ausland

Weltweit

Deutschland bei Google-Datenabfragen mit an der Spitze

In seinem aktuellen Transparency Report, einem regelmäßig herausgegebenen Bericht, listet Google unter anderem auf, welche Regierungen weltweit die Löschung von Inhalten verlangen und wie viele Anfragen zu Nutzerkonten sie stellen. Vor allem bei dem Wunsch, Google-Nutzende zu identifizieren, nimmt Deutschland demnach einen Spitzenplatz ein. Im ersten Halbjahr 2011 gab es im Vergleich zum Vorjahreszeitraum 38% mehr Anfragen nach Nutzerinformationen. Bislang hätten deutsche Behörden 1.060 Anfragen an Google geschickt, in denen es um die Identität von Account-InhaberInnen eines Google-Dienstes ging. Davon seien insgesamt 1.759 Nutzerkonten betroffen gewesen, denn eine Anfrage kann zu mehreren Konten führen. In 67% der Fälle habe man den Behörden ganz oder teilweise die verlangten Auskünfte erteilt.

Damit liegt Deutschland international auf dem fünften Platz. Mehr Datenanfragen stellten nur noch Großbritannien, Frankreich, Indien und die USA. Großbritannien beispielsweise hat 1.273 solcher Anfragen zu 1.443 Accounts gestellt, und die USA haben 5.950-mal um Daten gebeten, was 11.057 Accounts betraf. In den USA stieg damit die Zahl der Anfragen nach Nutzerdaten laut Google um 29%. Der amerikanische Datenschutz-Aktivist Chris Soghoian weist allerdings darauf hin, dass es Google gesetzlich untersagt ist, überhaupt zu erwähnen, wenn etwa die Bundespolizei FBI oder der Geheimdienst NSA solche Anfragen stellen. Bei bestimmten Ländern reagiert Google nicht auf eine Anfrage nach Nutzerdaten, schreibt Soghoian, beispielsweise bei den Regierungen von Iran, Vietnam, Libyen, Simbabwe. Dementsprechend ist die Liste der Länder mit Account-Anfragen relativ kurz. Das habe aber nur teilweise damit zu tun, schreibt er, dass Google Auskünfte verweigere, weil die Menschenrechte in diesen Staaten nicht ausreichend beachtet würden. Oft läge es wohl vielmehr daran, dass das Unternehmen in diesen Ländern keine lokalen Niederlassungen besitze und damit für Behörden nicht direkt ansprechbar sei (Biermann www.zeit.de 26.10.2011; www.heise.de 26.10.2011).

Europa

Streit über PNR-Datenabkommen mit den USA

Nach dem Scheitern eines ersten Vertragsentwurfes im Mai 2011 gab es schon nach der ersten Lektüre heftigen Widerstand aus mehreren Mitgliedstaaten der Europäischen Union (EU) gegen den nunmehr ausgehandelten Vertragstext zu einem Abkommen mit den USA über die Weitergabe der Daten von Fluggästen, den Passenger Name Recors (PNR). Dies konnte aber nicht verhindern, dass dieser von der verantwortlichen Innenkommissarin Cecilia Malmström am 17.11.2011 paraphiert wurde. Die Hauptkritik richtet sich gegen die vorgesehene Speicherdauer der Daten bis zu 15 Jahren. Zwar beginnen die Beratungen im Europaparlament über den geänderten Text des Abkommens erst, doch wurde sofort massiver Widerstand signalisiert. Jan Philipp Albrecht nannte die Vorlage eine „Mogelpackung“, die Substanz des zunächst gescheiterten Abkommens habe sich nicht geändert. Alexander Alvaro von den Liberalen nannte die Vorlage für „nicht zustimmungsfähig“. Die Sozialdemokratin Birgit Sippl sprach von einem „Flickenteppich“.

Malmström kalkuliert nach Ansicht von DiplomatInnen mit einem Doppeleffekt: Zum einen werde das Parlament am Ende zustimmen, weil die USA zu weiteren Zugeständnissen nicht bereit seien und die Daten bei einem Scheitern dieses Abkommen weiterhin nach den 2007 festgelegten und für Europa unvorteilhafteren Regeln abgreifen werden. Zum anderen wird im EU-Ministerrat in dieser Frage mit qualifizierter Mehrheit abgestimmt, so

dass sich schon eine größere Gruppe von Mitgliedsländern finden müsste, die den Vertrag blockiert. Angesichts des Wahlkampfs in den USA und der insgesamt nicht sonderlich guten transatlantischen Beziehungen wird das in Brüssel für eher unwahrscheinlich gehalten. Deutschland hat insofern mit seiner kritischen Position Schwierigkeiten; Kritik kam bei den ersten Beratungen der hohen Diplomaten der 27 Mitgliedsländer auch von Frankreich, den Niederlanden und Tschechien. Einige Länder legten „Prüfvorbehalte“ ein. Aber nur Berlin steht unter dem Druck eines Urteils des Bundesverfassungsgerichtes vom März 2010 zur „Vorratsdatenspeicherung“, wonach die Speicherung strengen Kriterien der „Verhältnismäßigkeit“ entsprechen muss, die im geänderten Abkommen nicht erfüllt sind. Die Kommission hat die deutsche Kritik mehrfach als „unfair“ zurückgewiesen. Der neue Text treffe, so Malmström, „sehr starke Vorkehrungen zum Schutz der Privatsphäre der europäischen Bürger“. Die Innen- und Justizminister wollten sich im Dezember 2011 mit dem Text auseinandersetzen, das Europaparlament (EP) im Januar 2012.

Zuvor hatte das EP am 27.10.2011 ein PNR-Abkommen mit Australien mit großer Mehrheit verabschiedet. Danach werden die PNR künftig fünfeinhalb Jahre lang in Australien gespeichert. Zu den 19 Passagierdaten, die Fluggesellschaften den australischen Behörden übermitteln müssen, zählen Adressen und Zahlungsinformationen, aber auch Speisewünsche und gegebenenfalls die bei der Reisebuchung verwendete IP-Adresse. Von der Speicherung ausgenommen sind lediglich sensible Daten wie Religion, Gesundheit und sexuelle Orientierung der Reisenden. Das EP verabschiedete das PNR-Abkommen mit 463 zu 96 Stimmen bei 11 Enthaltungen. Der fraktionslose österreichische EU-Abgeordnete Martin Ehrenhauser bemängelte den Entscheid als einen „schweren Rückschlag für die Glaubwürdigkeit des Parlaments als Wächter über die Bürgerrechte in Europa“. Sein Kollege Jan Philipp Albrecht von der grünen Fraktion im EU-Parlament nannte das Abkommen unverhältnismäßig. Die Fraktion prüfe gerichtliche Schritte, „um dieser grundrechtswidrigen Praxis einen Riegel vorzuschieben“ (www.heise.de 27.10.2011; Winter SZ 18.11.2011, 8).

Europa

Visa-Informationssystem nimmt Betrieb auf

Das Visa-Informationssystem (VIS) der europäischen Schengen-Staaten ist am 11.10.2011 in Betrieb gegangen. Zunächst kommt das System in den Botschaften und Konsulaten der beteiligten europäischen Länder in der „Anwendungsregion Nordafrika“ zum Einsatz (Ägypten, Libyen, Mauretanien, Marokko und Tunesien). Es soll bald auf den Nahen Osten und die Golfregion ausgeweitet werden. Personen, die in den Konsulaten dieser Region ein Visum für einen kurzfristigen Aufenthalt in einem der 25 europäischen Länder beantragen, müssen ihre biometrischen Daten (Fingerabdrücke und Lichtbild) abgeben, die für fünf Jahre im VIS, also in einer zentralen Datenbank der Visum-Antragsteller gespeichert werden. Gespeichert werden auch die Daten abgelehnter, annullierter und erneuerter, beziehungsweise verlängerter Visumanträge ebenso für jeweils fünf Jahre die Daten der einladenden Personen. Neben der zentralen Datenbank (C-VIS) existiert in jedem Schengenstaat eine „nationale Schnittstelle“ (N-VIS), über die Visumsbehörden und Strafverfolger Einsicht in die Datenbestände nehmen können. Unter bestimmten Umständen haben auch Europol und die nationalen Polizeien Zugriff. Bei der Einreise können Grenzbeamte die Identität der VisuminhaberIn anhand der Daten überprüfen. Mit dem System soll u. a. Identitätsdiebstahl verhindert und die Bearbeitsdauer bei Anträgen verkürzt werden. VIS sollte ursprünglich schon im Dezember 2009 starten; der Mitgliedsstaaten hatten aber wie beim Schengener Informationssystems (SIS) mit IT-Problemen zu kämpfen. Seinerzeit einigte man sich in der entsprechenden europäischen VIS-Verordnung von 2009, dass der Start „erst erfolgt, wenn sämtliche Schengen-Mitgliedstaaten rechtlich und technisch in der Lage sind, diese Verordnung umzusetzen.“ Dies sollte im März 2010 der Fall sein, konnte aber erst im Oktober 2011 realisiert werden.

Extra für VIS wurde 2008 das Forschungsprojekt BioDEV II ins Leben gerufen, das die Zuverlässigkeit der biometrischen Datenerfassung testen sollte. Dabei stellte sich heraus, dass die ersten 12.000 Datensätze unbrauchbar waren und die biometrische Erkennung nicht befriedigend funktionierte. Nach gründlichen Schulungen und Reinigungsmaßnahmen wurden bessere Ergebnisse erzielt. Dennoch wurde noch 2010 von einer Fehlerrate von 12 bis 16 % berichtet. Das Bundesinnenministerium betont, mit VIS würden die Antragsverfahren sowie die Kontrollen an den Grenzen verbessert und damit die Sicherheit im Hoheitsgebiet der Schengen-Staaten substanziell erhöht werden. Über die aktuellen Kosten von VIS liegen keine Angaben vor. Als der Europäische Rat sich 2004 für die Einrichtung von VIS entschied, wurden die Kosten auf 130 bis 200 Millionen Euro geschätzt (Borchers www.heise.de 11.10.2011; SZ 12.10.2011, 6).

Europa

Agentur für große IT-Systeme gegründet

Nach Zustimmung des EU-Ministerrats zu einem Kompromiss mit dem Parlament und der Kommission soll die „Agentur für große IT-Systeme“ (Agency for large scale IT systems) im Sommer 2012 ihre Arbeit aufnehmen. Die Behörde soll das Schengen-Informationssystem II (SIS II) und das Visa-Informationssystem VIS (s. o.) betreiben, wenn diese fertiggestellt sind. Außerdem wird sie die bislang bei der EU-Kommission angesiedelte Fingerabdruckdatenbank für AsylbewerberInnen und illegale EinwandererInnen (EURODAC) verwalten. Sie soll zudem, so die Direktive, künftig weitere IT-Projekte im „Raum der Freiheit, der Sicherheit und des Rechts“ übernehmen. Sitz der Agentur wird die estnische Hauptstadt Tallin sein. Entwicklung und operativer Betrieb finden in Straßburg statt; im österreichi-

schen Sankt Johann im Pongau gibt es eine Backup-Installation. An beiden Orten ist bereits die bisherige Schengen-Technik in Betrieb.

Geleitet wird die Behörde von einem Verwaltungsrat, dem je ein Vertreter aus den 27 EU-Mitgliedsstaaten, den assoziierten Ländern Island, Norwegen, Schweiz und Liechtenstein sowie zwei Vertreter der EU-Kommission angehören. Über welche Aspekte die assoziierten Staaten in diesem Rat entscheiden dürfen und wie sie an der Finanzierung der Behörden beteiligt werden, ist noch nicht endgültig geklärt. SIS II soll im ersten Quartal 2013 starten und dann bis zu 100 Millionen Datensätze verwalten können. Die Aufrüstung vom aktuellen Schengen-System, das zurzeit 35 Millionen Records speichert, begann 2006 und hat bislang mindestens 90 Millionen Euro gekostet (www.heise.de 12.09.2011).

Europa

Statewatch kritisiert EU-Strafverfolgung

Gemäß einer Analyse der britischen Bürgerrechtsorganisation Statewatch geht die zunehmende Kooperation zwischen Strafverfolgern in der EU auf Basis des „Prinzips der Verfügbarkeit“ nationaler Ermittlungsdaten zu Lasten der Grundrechte. Derzeit werden eine Reihe übergreifender IT-Systeme aufgebaut, um den Austausch von Informationen zwischen verschiedenen Sicherheitsbehörden zu erleichtern. Statewatch-Experte Chris Jones meint, dass es für eine begrenzte Kooperation in diesem Bereich sicher gute Gründe gibt. Die gegenwärtigen Versuche unterwanderten aber mit dem einfachen und systematischen Transfer großer Datenmengen eine Reihe vermeintlich von den EU-Gremien hochgehaltener Grundrechte. Entsprechende Gesetzgebungsverfahren zeigten wenig Sensibilität für den Schutz der Privatsphäre der BürgerInnen und seien allein auf die Wünsche von Polizei- und Justizbehörden ausgelegt.

Am weitesten gediehen sind dem Report zufolge die Arbeiten am Europäischen Strafregisterinformationssystem, das auch der EU-Datenschutzbeauftragte Peter Hustinx kritisiert hat. Das European Criminal Records Information System (ECRIS) soll es Ermittlern und Staatsanwälten erlauben, Informationen aus Strafakten der Mitgliedsstaaten zu ziehen, und so etwa bei einem neuen Verfahren auf bereits frühere Verurteilungen hinweisen. Für Jones ist das Konzept äußerst problematisch. Kennzeichen dafür seien „schwere Fehler beim Datenschutz, das Verlassen auf potenziell mangelhafte Maschinenübersetzungen und ein erhebliches Kontrolldefizit“. Darüber hinaus habe sich die Reichweite des Registers bereits über die ursprüngliche Planung hinausbewegt.

Das in Planung befindliche Polizeisystem EPRIS (European Police Records Index System) wird von Europol und einer Reihe von Mitgliedsstaaten entwickelt. Es soll Ermittlungsbehörden die Möglichkeit an die Hand geben, die Datenbanken der jeweils anderen Pendants nach personenbezogenen Informationen zu durchforsten. Einzelne EU-Länder hätten die Notwendigkeit des Registers und die Transparenz bei einschlägigen Beschlüssen zu seiner Errichtung hinterfragt. Hier sei höchste Wachsamkeit nötig, heißt es in der Studie.

Gemäß Jones stehen die Arbeiten an einer noch weitergehenden Austauschplattform für Strafverfolgungsbehörden, des Projektes einer „Information Exchange Platform“ (IXP), noch am Anfang. IXP setze auf einen zentralen Zugang zu allen Informationswerkzeugen und Datenbanken der europäischen Ermittler und zugehöriger Ämter. Eine entsprechende Empfehlung des Generalsekretariats des EU-Rates als zugriffsberechtigte Instanz deute auf einen deutlichen Wandel in der Art und Weise hin, in der Akten über Verdächtige und Verurteilte verbreitet würden und wem sie zur Verfügung stünden. Auch dieses Projekt müsse gemeinsam mit den beiden anderen Vorhaben unter Beobachtung gestellt werden, wozu Statewatch eine eigene Website freigeschaltet hat (Krempl www.heise.de 03.09.2011; die Studie ist unter http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf im Netz abrufbar)

Belgien

Pädophilie-Test für Priesteranwärter

Katholische Priesteranwärter müssen sich in Belgien künftig psychologischen Tests unterziehen, um späteren Kindesmissbrauch auszuschließen. Gemäß André Joseph Léonhard, dem Vorsitzenden der Bischofskonferenz, sollen unter den Seminaristen pädophile Neigungen aufgespürt werden: „Die Kirche muss die Kinder besser schützen.“ Die Männer würden „gescreent“. Dazu werde ein psychologisches Profil erstellt. Im Jahr 2010 musste der Bischof von Brügge, Roger Vangheluwe, wegen sexuellen Missbrauchs sein Amt aufgeben. Eine Untersuchungskommission erhielt Hunderte Zuschriften von Menschen, von Kirchenangehörigen misshandelt worden zu sein (SZ 21.09.2011, 9).

Frankreich

Copwatch stellt Polizisten an Internetpranger

Auf den Internetseiten von „Copwatch“ werden französische Gendarmen beschimpft – mit Name, Foto und Adresse und als Provokateure, Schläger, Alkoholiker oder Faschisten gescholten. Die französischen PolizistInnen und GendarmInnen werden zu Dutzenden mit Fotos auf der Internetseite „Copwatch-Nord-Ile-de-France“ unter Namens- und Adressangabe dargestellt, oft mit Porträtbildern, manchmal im Dienst, manchmal privat. Dabei stehen Kommentare wie: „Stratege der Hinterhalte und der Jagd auf die Armen“, „Zögert nicht zuzuschlagen“ oder „Erniedrigt die Einwanderer und behandelt sie wie Deppen“. Innenminister Claude Guéant will die Internet-Seiten nun teilweise sperren lassen. Die Veröffentlichung sei skandalös und gefährde die BeamtInnen. Den Betreibern gehe es nur darum, „zu stigmatisieren und die Polizisten samt ihren Familien zu stören“. Die Gewerkschaft Unité SGP Police kritisiert, Copwatch verbreite Slogans, die zum Widerstand gegen die Polizei aufriefen und so zur Gewalt aufstachelten. Ein Beamter, der

auf der Internetseite angeprangert wurde, fand kürzlich eine Gewehrkugel in seinem Briefkasten.

Die Copwatch-Betreiber rechtfertigen sich, sie wollten Missstände in der Polizei aufdecken und für Transparenz sorgen. Sie berufen sich auf ähnliche Initiativen, die in den USA seit den neunziger Jahren entstanden sind. Die französischen „Polizeibeobachter" gehen raffiniert vor, indem sie sich etwa auf Facebook als Freunde von PolizistInnen ausgeben und so an Fotos und persönliche Informationen kommen. Ein Polizeigewerkschafter meinte: „Manche Polizisten sind nicht vorsichtig genug, sie sollten besser darauf achten, was sie über sich in den sozialen Netzwerken verbreiten". Der Innenminister hat eine einstweilige Verfügung gegen französische Internet-Provider beantragt, um den Zugang zu einem Teil der Copwatch-Seiten sperren zu lassen. An die Betreiber von Copwatch-Nord-Ile-de-France selbst kommt das Ministerium nicht heran, weil die Seiten auf einem Server in den USA angesiedelt sind. Die französischen Geheimdienste behaupten, hinter Copwatch steckten linksradikale AktivistInnen. Die Internet-Provider wiederum argumentieren, sie seien nicht für den Inhalt der Seiten verantwortlich, sondern stellten nur eine Vermittlungstechnik zur Verfügung (Ulrich SZ 13.10.2011, 10).

Großbritannien

Netzkontrolle nach Unruhen: „Überwachen statt abschalten"

Beim Treffen von britischen Regierungsmitgliedern und Vertretern von Facebook, Twitter und BlackBerry Ende August 2011 blieb vieles vage. Nach Straßenunruhen in London und vielen anderen Städten in Großbritannien wurde eine intensive Debatte begonnen über die Ursachen im und die mögliche Folgen fürs Internet.

„Jeder, der diese grauenhaften Ereignisse gesehen hat, wird geschockt sein zu hören, wie sie mittels sozialer Netzwerke organisiert wurden." Diesen Worten wollte der britische Premier David Cameron schnell Taten folgen lassen. Bei dem Treffen sollte es um knallharte Maßnahmen gehen, um den Ordnungshütern Zugriff auf die Daten von „Krawallmachern" in den populären Kommunikationsplattformen zu verschaffen. Nur so, behauptete Cameron vorab, ließen sich Ausschreitungen in Zukunft im Keim ersticken. In Krisenzeiten solle womöglich der Zugang zu Social Media komplett blokkiert werden.

Bei dem Treffen anwesend waren Innenministerin Theresa May, Polizeichefs sowie Vertreter von Facebook, Twitter und des BlackBerry-Herstellers Research in Motion. Im Ergebnis verpufften die kraftstrotzenden Ankündigungen des Premiers: Das Thema Abschaltung von sozialen Netzwerken in Krisenzeiten stand gar nicht erst auf der Tagesordnung. Offensichtlich hatte sich die Marschrichtung geändert. Der stellvertretende Staatschef Nick Clegg begründete dies damit, dass man keinen „black out" von sozialen Medien im Stil des Iran oder Chinas unterstütze. Diese Idee sei in der Hitze des Gefechts geboren worden. Die Zusammenkunft sei sehr konstruktiv gewesen. Statt soziale Netzwerke abzuschalten, wolle sich die britische Polizei in Zukunft darauf konzentrieren sie besser zu überwachen.

Facebook erklärte anschließend: „Wir begrüßen die Tatsache, dass bei diesem Treffen die gemeinsame Kooperation für die Sicherheit der Bevölkerung zur Debatte stand und nicht das Verhängen von Sanktionen gegen Internetdienstleister." In einem offenen Brief an Theresa May hatten sich zuvor unter anderem Amnesty UK, Privacy International und die Open Rights Group dafür ausgesprochen, dass die Überwachung und Restriktion von Kommunikationsnetzwerken mit äußerster Vorsicht erfolgen müsse. Unbestritten ist, dass sich Online-Netzwerke während der Unruhen sowohl für Krawallmacher als auch für Ordnungshüter als nützliche Kommunikationsorgane erwiesen. Während die Unruhestifter versuchten, ihre Aktionen auf Facebook und Twitter bekannt zu machen und zu koodinieren, war die Polizei damit beschäftigt, die Aktivitäten der Krawallmacher im Auge zu behalten, um Ausschreitungen zu verhindern. So gelang es den Ordnungshütern, geplante Attacken auf das Westfield London Einkaufszentrum, die Oxford Street und das Olympia-Gelände zu verhindern.

Als problematisch erwies sich jedoch, dass die Behörden keinen Zugriff auf den bei britischen Teenagern besonders beliebten Messengerservice von BlackBerry hatten. 37% der jungen Leute im Königreich bevorzugen BlackBerry statt anderer Smartphones. BBM (BlackBerry Messenger) hat für sie längst die SMS ersetzt, denn es ist kostenlos und kann nicht mitgelesen werden. Die Tageszeitung Guardian berichtete, im Verlauf der Unruhen sei folgende Nachricht via BBM verschickt worden: „Kommt alle zum Oxford Circus. Brecht in Geschäfte ein und holt euch Zeug umsonst. Die Bullen können uns am Arsch lecken, wir schlagen zurück mit unseren Krawallen … wenn du einen Bruder siehst grüß ihn, wenn du einen Bullen siehst, erschieß ihn!" Der Guardian behauptet, 2,5 Millionen Tweets zum Thema analysiert zu haben. Demnach sei Twitter während der Unruhen in erster Linie zum Chatten und nicht als Protestorgan der Krawallmacher genutzt worden. Trotzdem stehen die Online-Netzwerke seit den Unruhen in der Schusslinie. Laut einer Umfrage der britischen Marketingagentur MBA sprachen sich 2.000 BritInnen für eine temporäre Sperre dieser Medien bei Krawallen aus. Es ist allerdings kaum zu erwarten, dass die britische Regierung nach der Kehrtwende dieses Thema noch einmal anfassen wird (Diebel www.taz.de 30.08.2011).

Irland

Regierung stellt Beichtgeheimnis in Frage

Die irische Regierung kündigte an, der Staat wolle das Beichtgeheimnis nicht mehr respektieren, wenn es um sexuelle Gewalt gegen Kinder geht. Um Kinder zu schützen, müsse jeder Missbrauchsverdacht zur Anzeige gebracht werden. Nach Ansicht von Ministerpräsident Enda Kenny versuche sich die Kirche per Sonderrecht der Aufklärung zu entziehen. Tatsächlich scheint der Vorstoß eher gegen die katholische Kirche gerichtet zu sein. Eine

Anzeigepflicht verhindert sexuelle Gewalt nicht; Täter würden ihre Taten eben nicht mehr beichten. Auch den Opfern würde sie wohl wenig dienen. Diese vertrauen sich jemandem oft nur an, wenn sie sich der Verschwiegenheit des Gesprächspartners sicher sein können.

Die katholische Kirche verteidigt ihr Geheimnis. Der irische Kardinal Sean Brady erklärte, dass die Kirche „auf keinen Fall" das Beichtgeheimnis aufweichen werde. Dieses gilt auch in der evangelischen Kirche und entspricht der Verschwiegenheitspflicht von ÄrztInnen, TherapeutInnen, SozialarbeiterInnen. Die Verschwiegenheit soll einen Raum des Intimen und Geschützten schaffen, in den niemand eindringen darf und in dem Hilfe und Schutz für Menschen in Not gewährt werden kann. Wer den Raum des Verschwiegenen bereitstellt, muss vertrauenswürdig sein. Insofern hat die katholische Kirche in Irland viel verloren, indem sie Priester schützte, die Kindern und Jugendlichen sexuelle Gewalt antaten. Dies sollte aber nicht dazu führen, dass die kulturelle Errungenschaft des Beichtgeheimnisses angetastet wird. Dieses ist seit 1215 im katholischen Kirchenrecht verankert (Drobinski SZ 31.08.2011, 4).

Polen

Innenministerium gibt Spähsoftware in Auftrag

Das polnische Innenministerium hat ein bisher illegales Schnüffelsystem in Auftrag gegeben. Mit dem Staatstrojaner sollen Polizei und Geheimdienst künftig unbemerkt in private Computer eindringen können, um dort vor allem Internet-Geldüberweisungen auszuspähen und dabei auch die von Banken verwendeten Verschlüsselungssysteme Proxy und zu Tor unterlaufen. Die Gesellschaft Blogmedia24 hatte Ende Oktober 2011 bei der Staatsanwaltschaft in Warschau eine Anzeige gegen die „Staatshacker" eingereicht. Das Strafgesetzbuch Polens (Art. 269b) sage ganz klar, dass weder die Polizei noch die Geheimdienste Polens das Recht hätten, Hackersysteme zum Ausspähen der Staatsbürger in Auftrag zu geben. Polens Innenministerium unter Jerzy Miller gab zu, dass es für einen Teil des in Auftrag gegebenen Hackersystems keine gesetzliche Grundlage gebe. Das neue Parlament solle aber in Kürze ein erweitertes Polizei- und Geheimdienstrecht verabschieden. Vorher würden die Staatstrojaner nicht eingesetzt. Sebastian Serwiak, der Abteilungsleiter für Öffentliche Sicherheit im Innenministerium, meinte: „Es ist nichts Besonderes dabei, dass etwas gebaut wird und die Legalisierung erst später kommt. Zuerst entstand das Auto. Und erst dann wurde das Verkehrsrecht geschaffen."

Schon bisher kann mit richterlicher Genehmigung ein privater Computer ausgespäht werden, wenn ausreichende Verdachtsmomente gegen die NutzerIn vorliegen. Die neue Software soll nun aber auch das Blockieren von Internetinhalten ermöglichen. Dieses Recht haben bislang ausschließlich die Inhaber der Server, auf denen sich die inkriminierten Internetseiten befinden. Das Chiffrier-System Proxy und das Netz Tor ermöglichen das anonyme Surfen im Internet, indem die ID-Adresse eines Computers verändert wird. Banken nutzen diese Dienste, um ihren KundInnen sichere Überweisungen im Internet zu ermöglichen. Auf Nachfrage verwies das Innenministerium auf Regelungen, die es erlauben – ohne Wissen der Telefonkunden – die Liste aller Verbindungen einer Person einzusehen sowie auf ein Gesetz, das Polizei und Geheimdienst das geheime Abhören und Abspeichern der Gespräche einer verdächtigen Person sowie das Anbringen von Wanzen erlauben. Zwar wäre in allen Fällen die Genehmigung durch ein Gericht notwendig. Doch in der Praxis werden Informationen von staatlichen Stellen und Telekom-Firmen als „öffentlich zugänglich" klassifiziert. Dies gilt auch für per GPS festgestellte Lokalisierungsdaten. Hier wird in der Praxis keine Genehmigung eingeholt. Sollte das Polizei- und Geheimdienstzusatzgesetz wie geplant vom neuen polnischen Parlament verabschiedet werden, könnten, so die Angst der Gesellschaft Blogmedia24, auch die durch ein Trojanersystem gewonnenen Informationen aus einem privaten Computer als „öffentlich zugänglich" klassifiziert und über Jahrzehnte gespeichert werden. Dass ihre Anzeige Erfolg haben könnte, bezweifelt der Strafrechtsprofessor Wlodzimierz Wrobel: „Prüfen kann man allenfalls, ob öffentliche Gelder zur Entwicklung eines Ermittlungssystems ausgegeben werden dürfen, für das es keine rechtliche Grundlage gibt" (Lesser www.taz.de 09.11.2011).

Slowakei

Geheimdienst bespitzelte JournalistInnen

Der stellvertretende Vorsitzende der liberalen Partei „Freiheit und Solidarität" (SaS) Lubomir Galko wurde am 23.11.2011 von der christdemokratischen slowakischen Ministerpräsidentin Iveta Radicova nach einer Serie illegaler Lauschaktionen des militärischen Geheimdienstes Vos gegen JournalistInnen von seinem Amt als Verteidigungsminister entbunden. Der Abhörskandal war zwei Tage zuvor durch Berichte der Zeitung Novy Cas aufgeflogen, der offenkundig Abhörprotokolle des Geheimdienstes zugespielt worden waren. Demnach wurden monatelang aus Telefonaten von drei JournalistInnen von Pravda und des Generaldirektors des TV-Nachrichtensenders TA3 auch private Informationen, etwa zur Gesundheit, zum Intimleben oder zu den finanziellen Verhältnissen, festgehalten. Pravda-Chefredakteurin Nora Sliskova: „Es ist schwer vorstellbar, dass das ohne Wissen oder direkte Anweisung des Verteidigungsministers geschehen konnte." Sie kündigte Strafanzeigen gegen die Verantwortlichen an. Der Militärgeheimdienst bestätigte die Aktion und erklärte, sie sei von einem Richter genehmigt worden und habe dem Verdacht krimineller Aktivitäten der Abgehörten gegolten.

Premierministerin Radicova erklärte dagegen, die Aktion stehe nicht im Einklang mit den Prinzipien des Rechtsstaates: „Unter keinen Umständen, ob legal oder illegal, kann ein Abhören von Journalisten durch Geheimdienste für uns zulässig sein." Zu der Meldung, sie selbst sei unter dem Codenamen „Die Dame" ein Opfer der Lauschangriffe, äußerte sie sich nicht.

Dies soll zu einer Zeit passiert sein, als sie gegen den Interessenkonflikt eines Staatssekretärs der SaS im Wirtschaftsministerium vorging, der dann abdanken musste. Der entlassene Minister Galko nannte den Bericht über die Abhöraktion eine Erfindung und behauptete, dass er in seiner gut einjährigen Amtszeit illegale Geschäftsmacherei und zweifelhafte Beschaffungsaufträge im Verteidigungsressort gestoppt habe. Den Vorwurf, die Regierungschefin sei abgehört worden, wies er als unwahr zurück. Die Affäre sei ein Racheakt von Geschäftemachern (Brill SZ 24.11.2011, 7; SZ 22.11.2011, 8).

Schweiz

Bwin gibt Zehntausende KundInnendaten weiter

Der internationale Online-Wettanbieter Bwin hat Zehntausende KundInnendaten an den Schweizer Adresshändler Hermes Direkt von Bwin-Kunden weitergegeben, der die Adressdaten verschiedenen Unternehmen zur Mietnutzung anbot. Die Daten stammten von Briefumschlägen, die Hermes Direkt von Bwin erworben hat. Der Wettanbieter bestätigte den Vorfall und behauptete, getäuscht worden zu sein. Demnach soll sich ein Hermes-Mitarbeiter als Briefmarkensammler ausgegeben haben. So habe er sich an Bwin geschickte Kundenbriefe besorgt. Zur Anzahl der weiter gegebenen KundInnendaten machte Bwin keine Angaben, die Presse berichtete unter Berufung auf interne Unterlagen von 110.000 übermittelten Adressen. Jürgen Wolff, Geschäftsführer von Hermes Direkt, widersprach der Darstellung von Bwin. Das Unternehmen habe genau gewusst, worum es bei dem Geschäft gehe. „Gier frisst Hirn“, sei das Credo bei solchen Geschäften. Bei Bwin habe Hermes Direkt „200 bis 300 Kilogramm Briefumschläge“ abgeholt, nicht alle seien allerdings mit einer Absenderadresse versehen gewesen. Auf der Hermes-Seite stehen 52.000 Adressdaten von deutschen Bwin-KundInnen zur Miete bereit – bei Nennung der Datenherkunft seien Mailings an diese KundInnen absolut mit dem Schweizer Datenschutzrecht vereinbar, behauptet Wolff.

Ein Bwin-Sprecher beteuerte gegenüber Medien, der Adresshändler habe sich als Briefmarkensammler ausgegeben und im April 2011 270 Kilogramm alte und leere Umschläge von BriefwettenkundInnen erworben. Davon gebe es allerdings nur noch „eine dreistellige Anzahl“ – mehrere Zehntausend Datensätze könnten auf diesem Weg kaum generiert worden sein. Das Unternehmen bedauere die Situation, gerade weil das Unternehmen im Internet Maßstäbe beim Datenschutz setze. Dass es keinen bewussten Adresshandel gegeben habe, sei schon daran abzulesen, dass Bwin für die Umschläge nur einige Hundert Euro erhalten habe (1,88 Euro pro Kilogramm). Der Wettanbieter hat nach eigenen Angaben seinen Anwalt damit beauftragt, rechtliche Schritte gegen Hermes zu prüfen (www.heise.de 26.09.2011, update 27.09.2011).

Schweiz

Bankdaten werden an die USA ausgeliefert

Die Großbank Credit Suisse kommt nach eigenen Angaben einer Aufforderung der Schweizer Regierung nach und gibt die geheimen Daten über 130 US-KundInnen preis. Auslöser der Aktion war ein Amtshilfegesuch der US-Steuerbehörde IRS. Diese verlangte Dokumente und Daten von KundInnen mit Vermögen in speziellen Finanzverhikeln. Schweizer Banken werden verdächtigt, bei Steuerhinterziehung geholfen zu haben (SZ 14.11.2011, 17).

Schweden

Zeitungen schaffen Anonymität für Internetkommentare ab

Als Reaktion auf die Anschläge von von Utøya und Oslo in Norwegen haben Anfang September 2011 drei große schwedische Zeitungen überraschend bekannt gegeben, die Möglichkeiten für anonyme Kommentare auf ihren Webseiten drastisch einzuschränken. Dagens Nyheter, größte Abo-Zeitung des Landes, schaltete seine Foren sogar ganz ab. Bis Mitte Oktober soll die Netzdebatte auf DN.se verstummen, teilte das Blatt mit. Dann werde man ein neues System mit schärferen Kontrollen einführen. Die Aktion, an der sich auch die großen Boulevardblätter Expressen und Aftonbladet beteiligten, sorgte für einen Aufschrei in der Netzgemeinde. Von „Zensur“ war die Rede. Anna Troberg, Vorsitzende der Piratenpartei, nannte die Entwicklung „beunruhigend und unglücklich“.

Schweden ist stolz auf seine lange Tradition der Meinungsfreiheit. Die Medien ließen ihre Foren bislang weit offen: Die NutzerInnen mussten meist nicht einmal eine E-Mail-Adresse angeben. Unflätiges versuchten die Redaktionen im Nachhinein zu löschen, kamen aufgrund der Meinungsflut damit aber oft nicht mehr nach.

Anders als in Deutschland gab es in Skandinavien nach den Anschlägen kaum politische Diskussionen um Netzanonymität; staatliche Einmischung in die Medien ist verpönt. Doch begann eine Debatte innerhalb der Branche, die nun in diese Selbstregulierung mündete. Diskutiert wurde über das Thema ohnehin schon länger, einige Lokalzeitungen hatten die Forenregeln bereits im Frühjahr 2011 verschärft. Bei Aftonbladet sollen sich die NutzerInnen nun künftig mit einem Facebook-Profil einloggen, um zu kommentieren. Damit soll die Anonymität eingeschränkt werden – obwohl es natürlich möglich bleibt, sich bei Facebook ein Pseudonym zuzulegen. Chefredakteur Jan Helin hofft dennoch, dass der Ton sich bessert, wenn man einen Namen nennen muss.

Die Idee hat Aftonbladet von seinem norwegischen Schwesternblatt Verdens Gang übernommen, das dieses System kurz nach den Anschlägen einführte und damit nach eigenen Angaben gute Erfahrungen macht. Expressen geht noch weiter: Dort sollen künftig alle Nutzerbeiträge von RedakteurInnen freigeschaltet werden. Chefredakteur Thomas Matsson erklärte in seinem Blog: „Das war kein einfacher Beschluss für eine liberale Zeitung. Das Medium ist zwar reif für das Publikum, aber das Publikum ist nicht reif für das Medium.“ Üble Personenangriffe

wolle er nicht länger tolerieren. Es sei auch nicht vernünftig, dass so gut wie alle Foren – selbst unter Berichten zu Wetter und Sport – von Leuten gefüllt würden, die gegen Einwanderung seien. Rassistische Kommentare nannten die Blätter als Hauptgrund für ihren Vorstoß. Troberg von der Piratenpartei räumte ein, dass die Netzdebatten teilweise aus dem Ruder laufen: „Einige überschreiten die Grenze und benehmen sich wie Schweine“. Die Reaktion hält sie dennoch für falsch: Statt Unerwünschtes zu verbannen, sollten die JournalistInnen lieber als „Gastgeber“ auftreten und mitdiskutieren: Ein Mensch, dem man gegenübertrete, werde sich „seltener wie ein Idiot verhalten, als ein Mensch um den sich niemand kümmert“ (Herrmann SZ 02.09.2011, 15).

USA

Verbrechensprognose per Computer

Die Polizei in Santa Cruz/Kalifornien versucht etwas, was immer wieder vergeblich angegangen wurde: Mit einer speziellen Software sollen Ort und Zeitpunkt von Straftaten vorhergesagt werden. Obwohl die Testphase noch lief, sprach der Polizist Zach Friend schon von einem Erfolg: Die Zahl der Einbrüche in der 60.000-Menschen-Stadt sei seit Juli um 16% gegenüber dem Vorjahreszeitraum gesunken. Die Polizei füttert die Computer mit Verbrechensstatistiken aus dem vergangenen Jahrzehnt und täglich aktualisierten Daten. Dann wird berechnet, welche Gegenden und Uhrzeiten etwa für Autodiebstähle oder Einbrüche besonders beliebt sind. Dahinter steckt die These, dass Kriminelle dazu neigen, ihre Tat am selben Ort und zur gleichen Zeit zu wiederholen, wenn sie einmal erfolgreich waren. Jeden Tag errechnet der Computer 10 „Hot Spots“, an denen Beamte Verdächtige beobachten und gegebenenfalls festnehmen. 7 Kriminelle seien so seit Juli 2011 verhaftet worden. Behörden in Los Angeles, Chicago und New York arbeiten bereits mit ähnlichen Programmen (Der Spiegel 41/2011, 96).

USA

Supreme Court stellt GPS-Überwachung in Frage

Der Supreme Court, das oberste US-Gericht hat bei einer Anhörung am 08.11.2011 die Möglichkeiten zur Überwachung von Verdächtigen mit GPS-Technologie skeptisch beurteilt. Besonders irritierte die Richter die Aussage eines US-Regierungsvertreters, dass auch ihre Autos ohne richterliche Anordnung monatelang mit einem Satellitenpeilsender verfolgt werden können sollten. Ob Washington ein solches Verfahren tatsächlich für verfassungsgemäß halte, wollte der Vorsitzende Richter John Roberts wissen. Michael Dreeben bejahte das für das Justizministerium, solange sich die Überwachung auf das öffentliche Straßenland beziehe. Dem Anwalt fiel es bei der gut einstündigen mündlichen Verhandlung nicht leicht, die Regierungslinie der nicht von einem Gericht kontrollierten GPS-Verfolgung zu verteidigen. Sechsmal fühlten sich die Verfassungshüter an den Roman „1984“ von George Orwell erinnert. Dreeben versuchte, das Anbringen von Peilsendern an Fahrzeugen als technische Fortsetzung klassischer Polizeiarbeit darzustellen. Ermittelnde dürften auch ohne das Plazet eines Richters Mülltonnen durchsuchen, Verbindungsdaten abrufen oder Verdächtigen rund um die Uhr folgen, erklärte der Regierungsvertreter. Einen besonderen Schutz durch die Verfassung genössen alle Handlungen in den eigenen vier Wänden oder innerhalb eines Autos. Was eine Person der Außenwelt mitteile, einschließlich ihrer Fortbewegung in der Öffentlichkeit, dürfe dagegen aufgezeichnet und verfolgt werden. Hier gälten geringere Erwartungen an die Privatsphäre.

Richter Samuel Alito gab zu bedenken, dass es mit vernetzten Computern sehr einfach geworden sei, enorme Datenbestände anzuhäufen. Man könne daher nicht sagen, dass sich mit der digitalen Technologie nichts verändert habe. Dreeben entgegnete, dass es nicht um die Rundum-Beschattung jedeR US-BürgerIn gehe. Es ging im konkreten Fall um einen Drogendealer, gegen den es starke Verdachtsmomente gegeben hat. Insgesamt schätzte er, dass Behörden wie das FBI die Satellitenpeilung bislang in einigen tausend Fällen eingesetzt hätten. Nicht zufrieden zeigten sich die Verfassungshüter auch mit den Ausführungen des Anwalts der Gegenseite, Stephen Leckar, der den zunächst wegen Drogenhandels verurteilten US-Bürger Antoine Jones vertrat. Ein Berufungsgericht hatte das Urteil der ersten Instanz gegen den Beschuldigten aufgehoben, da die Ermittler keinen gültigen Durchsuchungsbefehl zu dessen GPS-Verfolgung vorweisen konnten. Dies wollte wiederum das Justizministerium nicht hinnehmen und schaltete den Supreme Court ein. Die Richter monierten, dass Leckar ebenfalls keine klare Grenze zwischen gängiger Polizeiarbeit und einem unverhältnismäßigen Eingriff in die Privatsphäre Betroffener aufgezeigt habe. Den von ihm gemachten Vorschlag, eine GPS-Überwachung für einen Tag ohne Richtererlaubnis zur Bestätigung eines Anfangsverdachts durchführen zu können, hielten sie nicht für tragfähig. Mit einem Urteil ist im Frühsommer 2012 zu rechnen (Krempl www.heise.de 09.11.2011).

USA

DNA-Test für Todeskandidaten

Ein Gericht in den USA hat den zum Tode verurteilten Häftling Hank Skinner am 03.11.2011, sechs Tage vor seinem Hinrichtungstermin, DNA-Tests verweigert, mit denen er seine Unschuld beweisen wollte. Er gebe keinen Hinweis darauf, dass diese Tests Hank Skinner entlasten könnten, begründete das Bezirksgericht in Texas seine Entscheidung. Ein Geschworenengericht in Texas hatte Skinner 1995 des dreifachen Mordes für schuldig befunden. Er soll am Silvestertag 1993 seine damalige Freundin und deren 20 und 22 Jahre alten Söhne in ihrem Haus getötet haben. Skinner gibt zu, zur Tatzeit im Haus gewesen zu sein, bestritt aber bis zuletzt seine Tat. Die von ihm geforderten Gentests an Beweismitteln vom Tatort, mit denen er nachweisen wollte, dass

Spuren an den Mordwerkzeugen nicht von ihm stammen, sondern auf einen anderen Täter hinweisen, hat die texanische Justiz seit mehr als einem Jahrzehnt immer wieder abgelehnt.

Der Journalistik-Professor der Northwestern University, David Protess, hat mit Studierenden den Fall Skinner über Jahre untersucht und kam zu dem Schluss, dass DNA-Tests an Skinner, verglichen mit solchen an den Opfern, den Todeskandidaten vom Vorwurf des Mordes entlasten würden. 1999, als DNA-Analysen allgemein verfügbar waren, ließ ein Gericht die Haare untersuchen, die am Tatort gefunden wurden. Als die Testergebnisse feststellten, dass keines der Haare von Skinner stammte, wurden alle weiteren Untersuchungen gestoppt. Zwei Jahre später verabschiedete Texas ein Gesetz, das DNA-Analysen nur dann zulässt, wenn die Ergebnisse die Unschuld des vermeintlichen Täters beweisen würden. Trotz des restriktiven Gesetzes konnte seitdem die Unschuld von 45 zu Unrecht Verurteilten bewiesen werden. Nach vier vorangegangenen Aufschüben sollte die Vollstreckung am 0911.2011 stattfinden. Zwei Tage vor der Vollstreckung ordnete dann das texanische Berufungsgericht an, den Antrag der Anwälte von Skinner auf Zulassung der DNA-Proben zu prüfen Das Berufungsgericht befand jetzt, dass sich die Gesetzgebung zu DNA-Proben mehrfach geändert habe, was bisher nicht berücksichtigt worden sei (SZ 05./06.11.2011, 14; KN 05.11.2011, 13; Häntzschel SZ 07.11.2011, 10; SZ 10.11.2011, 9).

USA

Tochter stellt prügelnden Vater im Netz bloß

Die heute 23jährige Tochter Hillary des texanischen Familienrichters William Adams stellte ihren Vater im Internet bloß, indem sie ein Video aus dem Jahr 2004 ins Netz stellte, wo zu sehen ist, wie der Vater acht Minuten lang seine damals 16 Jahre alte Tochter mit einem Gürtel schlägt. Das Video wurde millionenfach angeklickt. Die Tochter begründete ihre Veröffentlichung damit, ihr Vater brauche Hilfe. Dieser erklärte den Medien, er habe seine Tochter damals einfach „disziplinieren“ wollen (SZ 04.11.2011, 12).

USA

Scientology spioniert Filmemacher aus

Trey Parker und Matt Stone, die Macher von „South Park“, produzierten eine 2005 ausgestrahlte Episode mit dem Titel „Trapped in the closet“, in der sie sich derb über Scientology lustig machten. Während Scientology in Deutschland als Sekte öffentlich in der Kritik steht, wird die Organisation als autoritäre Religion in den USA weitgehend akzeptiert. Das ändert nichts daran, dass die Kirchenbosse auch in den USA Kritik nicht witzig finden, wie jetzt der Scientology-Aussteiger Marthy Rathburn in seinem Blog offenlegte. Rathburn dokumentiert in E-Mails, wie die Geheimdienstorganisation von Scientology, das „Office of Special Affairs“ (OSA), versuchte, Details aus dem Privatleben von Parker und Stone auszuspionieren. Das OSA ordnete danach an, den Müll der South-Park-Mitarbeiter zu durchwühlen, um „Telefonrechnungen, Kontoauszüge, private Briefe“ zu finden, in der Hoffnung, dabei auf „Schwächen“ zu stoßen, die man zur Einschüchterung nützen könne (SZ 31.10./01.11.2011, 17).

Kanada

Regierung will Internet schärfer überwachen

Kanadische DatenschützerInnen, BürgerrechtlerInnen, AkademikerInnen, SicherheitsexpertInnen und weitere Unterzeichnende wenden sich in einem offenen Brief an den kanadischen Ministerpräsidenten Stephen Harper gegen Pläne der Regierung, die Befugnis der Behörden zur Telekommunikationsüberwachung auszuweiten. Mit den geplanten Gesetzen würden zum Beispiel Internetprovider oder Anbieter sozialer Netzwerke zu Werkzeugen der Ermittler gemacht, schreiben die bürgerrechtlichen Organisationen und ExpertInnen und warnen vor Auswirkungen auf die Grundrechte. Die Watchdog-Gruppe „Open media.ca“, die den offenen Brief mit unterzeichnete, startete im Zusammenhang mit den geplanten Gesetzen den Aufruf „Stop Online Spying“. Über 45.000 Menschen hatten bis Ende August 2011 unterschrieben, um ihren Protest zum Ausdruck zu bringen.

Das Vorhaben der Regierung sehe keine ausreichenden Kontrollmöglichkeiten und Rechtsmittel vor, um einen Missbrauch zu verhindern. Gemäß dem Gesetzesentwurf sei für die Enthüllung einer Identität im Netz keine richterliche Genehmigung erforderlich und Daten dürften von Internet-Providern angefordert werden, und zwar nicht nur Name, Adresse, Telekommunikationsnummern und IP-Adressen, sondern auch Standorte von Handys und GPS-Geräten, Fotos und Kommentare in Sozialen Netzwerken. Behörden seien über durchgeführte Überwachungsmaßnahmen nicht berichtspflichtig. Unternehmen sollen die Daten über Nutzende länger speichern, wenn eine Behörde dies möchte – auch ohne richterlichen Beschluss. Die KritikerInnen verweisen in diesem Zusammenhang auf ähnliche Regelungen des US-amerikanischen Patriot Act, die als verfassungswidrig einzustufen seien.

Die nationale Datenschutzbeauftragte Jennifer Stoddart hatte gemeinsam mit regionalen Datenschutzbehörden bereits im März 2011 einen Brief ans Ministerium für Öffentliche Sicherheit in Kanda geschrieben: „Zusammen genommen würden die Gesetze … die Privatrechte der Kanadier substanziell schwächen“. Die Gesetzesänderungen würden Ermittlern mehr Macht geben, um digitale Informationen zu verfolgen, zu suchen und in Besitz zu nehmen. Das alles, so kritisieren die DatenschützerInnen, würde darüber hinaus nicht mit einer verstärkten unabhängigen Kontrolle der Behörden einhergehen. „Mit derartigen Bedenken über dieses gruselige Spionage-Modell muss die Regierung erkennen, wie problematisch ihre Pläne sind“, sagt Tamir Israel, Anwalt an der „Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic“ auf „Open me-

dia.ca“. Israel hofft, dass die Regierung noch einmal umdenkt – oder wenigstens mehr Zeit einräumt für eine ordentliche Anhörung im Parlament.

Die konservative Regierung unter Harper hat die Entwürfe für die Sicherheitsgesetze nach ihrem Sieg bei den vorgezogenen Neuwahlen im Juni 2011 mit dem Versprechen eingebracht, sie innerhalb von 100 Tagen durchs Parlament zu bringen. Zeit für eine Expertenanhörung im Abgeordnetenhaus bleibt dabei nicht. Die KritikerInnen rieten eindringlich davon ab, das Vorhaben ohne eine sorgfältige Prüfung seiner möglichen Auswirkungen bereits Anfang September zu verabschieden. Ein Sprecher des kanadischen Justizministers Rob Nicholson hatte zuvor gegenüber dem Sender CBC erklärt, dass die Initiative ausreichend Vorkehrungen zum Datenschutz enthalte. Der technische Fortschritt der vergangenen zwei Jahrzehnte habe die einschlägigen Behörden vor Schwierigkeiten gestellt, die Sicherheit der KanadierInnen aufrechtzuerhalten, meinte der Regierungsvertreter. Bestehende Sicherungen der Privatsphäre im nationalen Strafgesetzbuch würden beibehalten oder gar erweitert. Ohne richterliche Anordnung könne die Polizei keine Informationen erhalten (Krempl www.heise.de 22.08.2011; Havertz www.taz.de 24.08.2011; timestranscript.com 21.09.2011).

Mexiko

Anonymous erklärte kurzzeitig Drogenkartell den Krieg

Im September 2011 erschien ein Mann mit Guy-Fawkes-Maske auf YouTube, der als Mitglied der Hacker-Organisation Anonymous der mächtigsten Killerbande Mexikos den Cyberkrieg erklärte: Er würde die Daten von Polizisten, Politikern, Reportern und gar Taxifahrern, die die besonders brutalen „Los Zetas“ gegen Schmiergeld unterstützten, ins Internet stellen, wenn ein entführter Online-Aktivist nicht sofort freigelassen werde. Diese Veröffentlichung könne, so der Hacker, die Folge haben, dass die enttarnten Freunde der Drogenmafia möglicherweise mit dem Tod rechnen müssen. Am 31.10. sagten die Hacker dann aber ihre „Operation Kartell“ wieder ab. Das Video hatten bereits Hunderttausende gesehen, Nachrichtensender auf der ganzen Welt hatten es ausgestrahlt. Twitter-User @Sm0k34n0n schrieb: „Wir können das Leben unserer Kameraden nicht gefährden“ Ciménez SZ 02.11.2011, 12).

Syrien

Dissidentenüberwachung mit deutscher Technik

Der syrische Geheimdienst setzt bei der Überwachung der seit über viele Monate andauernden Proteste offenbar Technik der deutschen, zur Sohos-Gruppe gehörenden Firma Utimaco aus Oberursel ein. Das Unternehmen verwies darauf, keine Produkte direkt an das staatliche Unternehmen Syrian Telecommunications Esthablishment verkauft zu haben. Man habe die italienische Firma Area beliefert, mit der man seit Jahren zusammenarbeite. Dass diese an das Assad-Regime weiterverkauft habe, könne man nicht bestätigen. Neben der Utimaco-Software, die abgehörte Telekommunikationsleitungen mit den Rechnern in einem Überwachungszentrum verbindet, soll auch Speichertechnik und Software zur Mail-Archivierung der US-Firma NetApp zum Einsatz kommen. Von dem französischen Unternehmen Qosmos stammt nach Presseberichten die Technik zur Überwachung der Kommunikationsnetze. Die Hersteller sollen niemals direkt an Syrien geliefert haben, sondern immer nur an Area. Das fertige System ermögliche es Sicherheitsbeamten, Zielpersonen und ihre Kommunikation in Echtzeit zu verfolgen. Angeblich bezahlt Syrien für die bereits 2008 beauftragte Anlage rund 13 Millionen Euro.

Der Geschäftsführer von Area wollte zu den Details des Vertrags keine Stellung nehmen. Das Unternehmen halte sich an alle Gesetze und Exportbestimmungen. Die von der EU verhängten Sanktionen gegen Syrien betreffen nur den Verkauf von Waffen und das Eigentum syrischer Funktionäre. Schon im April 2011 hatte das Europäische Parlament schärfere Regeln für den Export von Überwachungstechnik gefordert. Bis zu einer Klärung der Vorwürfe habe Utimaco die Zusammenarbeit mit Area gestoppt. Vorangegangen war die Aufdeckung durch Hacker, dass bei der syrischen Telekom u. a. auch US-amerikanische Überwachungstechnik im Einsatz ist. Über die Verwendung von Utimaco-Software berichtete am 04.11.2011 der Wirtschaftsdienst Bloomberg unter Berufung auf Unterlagen und Insider. Der deutsche Linken-Bundestagsabgeordnete Andrej Hunko hatte schon 14 Tage zuvor die Bundesregierung nach Exporten deutscher IT-Firmen in Diktaturen und autokratische Regime gefragt und Utimaco benannt: „Diese Überwachungstechnik ist ein zentraler Teil der Repression in vielen Staaten; deshalb brauchen wir dafür endlich eine effiziente Ausfuhrkontrolle“ (Der Spiegel 45/2011, 18; www.heise.de 06.11.2011).

Japan

Neuer Hackerangriff auf Sonys Online-Dienste

Sonys Online-Dienste wurden erneut Ziel eines groß angelegten Hackerangriffs. Der japanische Elektronik-Riese teilte mit, dass die Angreifer auf breiter Front versucht hätten, in Nutzerkonten bei Sonys Online-Diensten einzudringen. Betroffen seien zwischen dem 07. und dem 10.10.2011 das Playstation Network (PSN), das Sony Entertainment Network (SEN) und Sony Online Entertainment (SOE) gewesen. In rund 93.000 Fällen sei es gelungen, in Konten einzudringen; diese seien vorerst gesperrt worden. 60.000 Accounts bei PSN/SEN seien betroffen und 33.000 bei SOE. Man werde die InhaberInnen der Konten per Mail informieren, eine Reaktivierung der Accounts erfordere ein Zurücksetzen der Zugangsinformationen mit sicheren Passwörtern. Kreditkarten-Informationen seien aber nicht in Gefahr, versicherte Sony, auch sei nur bei einem geringen Teil der kompromittierten Accounts vor der Sperre zusätzliche Aktivität festgestellt worden.

Gemäß den ersten Erkenntnissen kamen bei dem Angriff Passwort-Informationen zum Einsatz, die an anderer Stelle entwendet worden sind. Die Daten seien aus anderen Passwortlisten anderer Unternehmen, Webseiten oder Quellen gekommen. Viele Menschen nutzen dasselbe Passwort bei verschiedenen Onlinediensten. Werden die Schutzmaßnahmen einer Firma geknackt, so sind auch andere Nutzerkonten in Gefahr. Die Angriffe hätten in Versuchen bestanden, gültige Accounts durch Ausprobieren mit langen Listen von Anmelde-IDs und Passwörtern zu finden. Im September 2011 holte sich Sony den ehemaligen ranghohen Beamten der US-Heimatschutzbehörde Philip Teitinger als IT-Sicherheitschef. Dieser betonte, der Einbruchversuch sei nur bei 0,1 % der Nutzerkonten erfolgreich gewesen.

Im April 2011 hatten es Unbekannte geschafft, sich Zugang zu Daten von mehr als 100 Millionen KundInnen von Online-Diensten des Konzerns zu verschaffen (DANA 2/2011, 80 ff.). Diese Angriffe hatten Sony zutiefst erschüttert. Nach dem ersten Einbruch gelang es den Angreifern trotz allen Anstrengungen des Konzerns über Wochen immer wieder, in Websites oder Netzwerke von Sony einzudringen. Für Sony war es eine teure Erfahrung: Der Konzern musste mehrere Online-Dienste wie das Playstation Network zeitweise vom Netz nehmen, die Sicherheitsarchitektur wurde von Grund auf erneuert (www.heise.de 12.10.2011; SZ 13.10.2011, 23).

Südkorea

Daten von Internet-Spielen geklaut

In Südkoera wurden Daten von 13 Millionen AbonnentInnen eines Internet-Spiels der im Land neben NVsoft führenden Internet-Unterhaltungsfirma Nexon Korea gestohlen. Die zuständige Aufsichtsbehörde teilte am 24.11.2011 mit, Hacker hätten sich Namen, Ausweisnummern und die Passwörter beschafft. Die Hacker sollen keine Informationen über finanzielle Transaktionen oder Kontonummern erlangt haben. Auch die AbonnentInnen im Ausland seien nicht betroffen. Der Vorfall ist der umfangreichste, seit Juli 2011 die Daten von 35 Mio. Nutzenden eines Internetportals von Sk Comms gehackt wurden (DANA 3/2011, 128). Die Spur führte damals nach China, dem im Jahr 2011 u. a. auch die Hackerangriffe auf US-Rüstungsfirmen wie Lockheed oder auf das Google-Mailprogramm angelastet werden (SZ 28.11.2011, 20).

Technik-Nachrichten

Smartphone-Bewegungssensoren analysieren Tippverhalten

Moderne Smartphones sind in der Lage, Texte zu entschlüsseln, die an einem nahelegenen Computer getippt werden. Patrick Traynor und Henry Carter vom Georgia Institute of Technology platzierten ein iPhone4 neben einer gängigen Computertastatur und erfassten mit Hilfe der im Handy eingebauten Beschleunigungssensoren die Vibrationen der Tastatur beim Schreiben. Das Handy registrierte dabei nicht einzelne Buchstaben, wohl aber Kombinationen von Anschlägen, für die jeweils die Position der Erschütterung auf der Tastatur (links – rechts) und die Entfernung zueinander erfasst wurde. Diese Abfolgen wurden mit einem elektronischen Wörterbuch abgeglichen, das rund 58.000 Wörter enthielt. Bis zu 80% eines getippten Textes konnten die Computerwissenschaftler auf diese Weise korrekt entziffern. Am zuverlässigsten waren die Ergebnisse, wenn das Handy nicht weiter als 7,5 Zentimeter von der Tastatur entfernt lag und die Wörter mindestens aus drei Buchstaben bestanden.

Die Beschleunigungssensoren eines Smartphones sollen primär erkennen, wie die NutzerIn ihr Telefon hält. Weil sie aber sehr sensibel sind, gibt es Handyspiele, die über Bewegungen der Nutzenden gesteuert werden. Anders als bei Handykamera, Mikrofon oder GPS-Ortung fragen entsprechende Apps die Nutzenden nicht, ob die Sensoren verwendet werden dürfen. So könnte eine Trojaner-App eingeschleust werden. Trayner meint: „Die Wahrscheinlichkeit, dass jemand auf diese Weise abgehört wird, ist derzeit gering.“ Wenn es aber jemand ernsthaft versuche, sei es möglich. Die Gefahr sei jedoch zu vermeiden, indem man sein Handy ausreichend weit weg von der Tastatur ablegt (SZ 20.10.2011, 20).

Martkforschung und Marketing per Gesichtsanalyse

Videokameras erfassen die Blicke ins Schaufenster von potentiellen KundInnen und eine Software ermittelt Alter und Geschlecht. Nach Feststellung von Geschlecht und Alter wird auf einem Bildschirm im Schaufenster ein Clip abgespielt, der z. B. für eine Biermarke wirbt, die sich an junge Männer richten soll. In den USA sind solche Formen der Marktforschung schon Realität. Das New Yorker Unternehmen Immersive Labs bietet ein entsprechendes System zur Gesichtsanalyse an, dessen Software in Echtzeit feststellen können soll, wer da gerade vor

dem Schaufenster steht: Die Software soll zuverlässig das Geschlecht, das ungefähre Alter, die Verweildauer und die Aufmerksamkeit der PassantInnen einschätzen. Immersive Labs will zudem den Ladenbesitzenden eine Publikumsstatistik anbieten, wie sie von Facebook-Fanseiten bekannt ist: Wie viele Frauen, wie viele Männer welcher Altersgruppe sind wann vor dem Bildschirm stehen geblieben? Die Software soll seit November 2011 in Los Angeles, San Francisco und New York zum Einsatz kommen. Das New Yorker Unternehmen ist einer von vielen Anbietern, die derzeit solche Systeme für Publikumsanalysen in physischen Räumen anbieten.

Viele Firmen arbeiten daran, mit derartigen digitalen Analysewerkzeugen die Realwelt zu erfassen. In Chicago haben gut 50 Bars ein Gesichtsanalysesystem des Unternehmens Scenetap installiert; die Software gibt auf einer Website an, wie hoch derzeit das Durchschnittsalter der BesucherInnen und wie das Frauen-Männer-Verhältnis ist. Das Kasino-Shopping-Hotel Venetian in Las Vegas nutzt laut Presseberichten Digital-Werbeplakate mit integrierter Publikumsanalyse. Adidas und der Lebensmittelkonzern Kraft wollen noch im Jahr 2011 solche beobachtende Werbung in US-Ladengeschäften testen. Wie zuverlässig Software allerdings das Geschlecht von Fotografierten im Schummerlicht von Bars erkennen kann, hängt von den eingesetzten Algorithmen ab. Da nicht bekannt ist, welche Verfahren Scenetap einsetzt, ist ein Urteil nicht einfach.

Der Informatiker Ralph Gross von der Carnegie Mellon University führte aus, was generell mit den heute verfügbaren Algorithmen zur Gesichtsentdeckung und -analyse umsetzbar ist: Gesichter werden generell auch in schlechten Lichtverhältnissen gut entdeckt, oft mit einer Trefferquote von 90 Prozent und mehr. Geschlechtserkennung funktioniert auch nachweislich gut, in einigen Studien wurden Trefferquoten von nahezu 90 Prozent erreicht. An der Zuordnung von entdeckten Gesichtern zu Altersgruppen arbeiten Forschende erst seit fünf Jahren intensiv, diese Aufgabe ist schwieriger zu lösen, die Trefferquoten sind derzeit niedriger als bei der Geschlechtserkennung. Es gibt mehrere Verfahren, die Aufmerksamkeit messen, zum Beispiel ob eine Person frontal zum Bildschirm steht oder wohin sie blickt; Letzteres ist erheblich schwieriger zu analysieren.

Anbieter dieser Analyseprogramme betonen, dass ihre Systeme nicht die Identität der Gefilmten feststellen. Die Software erkenne nur, ob gerade Gesichter gefilmt werden, nicht wem das Gesicht jeweils gehört. Der Begriff Gesichtsdetektion und -analyse ist für solche Verfahren treffender. Die Software Shore des Fraunhofer-Instituts für Integrierte Schaltungen (IIS) kann von Aufnahmen auf Altersgruppe, Geschlecht, Gesichtsausdruck (fröhlich, traurig) schließen. Außerdem analysiert das Programm die Position von Augen, Mund und Nase, die Neigung und Drehung des Kopfes, und wie weit Augen und Mund geöffnet sind. Fraunhofer-Forscher Jens-Uwe Garbas betont: „Eine Erkennung von Personen durch einen Abgleich mit einer Datenbank ist bei unserem Verfahren ausdrücklich nicht möglich.“ Außerdem würde die Fraunhofer-Software keine Daten speichern, durch die man auf einen bestimmten Nutzer rückschließen könne. Auf die Frage, wie schwierig es sei, entsprechende Erkennungsfunktionen nachzurüsten, antwortet Garbas: „Das kommt natürlich auf das System an.“ Da es sich bei Shore um ein Detektionsverfahren handele, sei das nur mit erheblichem Aufwand möglich.

Unbestreitbar lässt sich die für Gesichtsdetektion aufgebaute Infrastruktur auch zur Gesichtserkennung nutzen. Wie nah diese Einsatzszenarien einander sind, zeigt das japanische Unternehmen NEC. Die Firma ist nach eigenen Angaben führend auf dem Markt der biometrischen Lösungen – der Marktanteil liegt bei über 60 Prozent. NEC liefert Überwachungslösungen für Flughäfen. NEC wirbt in diesem Zusammenhang auch für die eigene Gesichtserkennungssoftware. Sie könne „Sicherheitsleute benachrichtigen, wenn Reisende als Personen identifiziert werden, die auf einer Beobachtungsliste registriert sind“. Außerdem könne ein System aus Überwachungskameras, Gesichtserkennungssoftware und Porträtdatenbanken auch nach Kriterien durchsucht werden wie „Kleidung in bestimmten Farben, Accessoires wie Gehstöcke, Geschlecht, Alter und Rasse“. NEC bietet vergleichbare Technologie auch zur Marktforschung an. Die Software FieldAnalyst wertet Video-Feeds von Überwachungskameras aus, um festzustellen, welche Zielgruppen zu welcher Zeit in welchen Bereichen etwa eines Einkaufszentrums zu finden sind. Die Software kann laut NEC-Eigenwerbung Altersgruppen, Geschlecht, Aufenthaltsdauer an bestimmten Orten und Besucherzahlen erfassen – personenbezogene Informationen der Fotografierten würden dabei nicht gespeichert.

Trotz dieser Beteuerungen ist klar, dass es leichter ist, vorhandene Gesichtsanalyse-Infrastruktur mit Erkennungsprogrammen aufzurüsten, als ein Überwachungssystem neu aufzubauen. Hierauf verwies der Informatiker Ralph Gross von der Carnegie Mellon University: „Wenn die Infrastruktur für die Aufnahme, die Bildübertragung und Ergebnisübertragung installiert ist, könnte nur ein Software-Upgrade nötig sein, um eine Identifizierungsfunktion nachzurüsten.“ Datenbanken, über die man Gesichtern Namen zuordnen kann, sind heute schon frei verfügbar. Bei Facebook sind zum Beispiel die Namen und die als Porträtfoto eingestellten Aufnahmen frei zugänglich. Ralph Gross hat mit KollegInnen von der Carnegie Mellon University in mehreren Versuchen nachgewiesen, dass es allein mit Hilfe der Facebook-Datenbank und gängiger Gesichtserkennungssoftware möglich ist, in Echtzeit den Namen fotografierter Personen herauszufinden. Derzeit verhindert allein die verfügbare Rechenkraft, dass man beispielsweise das Porträt eines Unbekannten mit allen Facebook-Profilen in einem Land abgleichen kann. Auf die Frage, wie schnell sich das ändern wird, meint Gross: „Es ist eher eine Frage von wenigen Jahren, bis das möglich ist, zumindest auf Großstadt-Ebene.“ Vielleicht werden dann die Stylingtipps gegen Gesichtserkennung, wie sie der Künstler Adam Harvey gibt, in naher Zukunft in Ratgebern von Datenschützern auftauchen (Litschka www.spiegel.de 17.11.2011).

Rechtsprechung

EuGH

Klagen wegen Internet-Persönlichkeits-verletzungen beim Wohnsitzgericht

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 25.10.2011 entschieden, dass bei Verletzungen von Persönlichkeitsrechten durch Inhalte auf einer Website (Texte, Bilder, Videos …), die vom Ausland aus ins Internet gestellt wurden, im Inland geklagt werden kann (Az. C-509/09 und C-161/10). Ausgangspunkt waren Klagen in Deutschland und Frankreich. Zwei Brüder wurden damals in Deutschland wegen Mordes verurteilt. Eine österreichische Gesellschaft berichtete über diesen Rechtsstreit mit voller Namensnennung. Die Brüder wollten Unterlassung fordern, doch von der Gesellschaft wurde die internationale Zuständigkeit des BGH angezweifelt. In Frankreich war der Schauspieler O. Martinez vor das Tribunal de Grande Instance de Paris gezogen, weil die britische Zeitung Sunday Mirror (MGN) einen in Englisch verfassten Artikel in Wort- und Bildform im Internet veröffentlichte. In diesem Artikel wurde über private Details berichtet. Martinez und sein Vater rügten eine Verletzung ihres Privatlebens sowie des Rechts am eigenen Bild. MGN meinte, das Tribunal de Grande Instance sei nicht zuständig, da kein hinreichend enger Bezug zwischen der Veröffentlichung und einem Schaden in Frankreich dargestellt wurde.

Der EuGH entschied nun, dass die Opfer von mittels des Internets begangener Persönlichkeitsverletzungen wegen des gesamten entstandenen Schadens die Gerichte ihres Wohnsitzmitgliedstaats anrufen können. Der Betreiber einer Website, für die die Richtlinie über den elektronischen Rechtsverkehr gilt, darf jedoch in diesem Staat keinen strengeren als den im Recht seines Sitzmitgliedstaats vorgesehenen Anforderungen unterworfen werden. Ebenso kann ein Gericht jedes Mitgliedstaates angerufen werden, in dessen Hoheitsgebiet ein im Internet veröffentlichter Inhalt zugänglich ist oder war. Logisch und sinnvoll ist hierbei allerdings die Einschränkung, dass dann nur über den Schaden entschieden werden kann, der in dem jeweiligen Land entstanden ist. Bei Klagen im „eigenen“ Land des Opfers kann vollumfänglich über den gesamten Schaden entschieden werden. Der Urheber der im Internet veröffentlichten Inhalte kann aber auch in seinem eigenen Land verklagt werden (Wagenknecht www.rechtambild.de 27.10.2011).

BGH

Videokamera in Klingelanlage erlaubt

Der Bundesgerichtshof hat mit Urteil vom 08.04.2011 entschieden, dass der nachträgliche Einbau einer Videoanlage im gemeinschaftlichen Klingeltableau gemäß § 22 Abs. 1 WEG verlangt werden kann, wenn die Kamera nur durch Betätigung der Klingel aktiviert wird, eine Bildübertragung allein in die Wohnung erfolgt, bei der geklingelt wurde, die Bildübertragung nach spätestens einer Minute unterbrochen wird und die Anlage nicht das dauerhafte Aufzeichnen von Bildern ermöglicht (Az. V ZR 210/10).

Die theoretische Möglichkeit einer manipulativen Veränderung der Anlage rechtfertigt nicht die Annahme einer über das Maß des § 14 Nr. 1 WEG hinausgehenden Beeinträchtigung. Ein Nachteil liegt erst vor, wenn eine Manipulation aufgrund der konkreten Umstände hinreichend wahrscheinlich ist. Der nachträgliche Einbau einer Videokamera am Klingeltableau der Wohnanlage ist eine bauliche Veränderung des gemeinschaftlichen Eigentums, die nur beschlossen oder verlangt werden kann, wenn jede WohnungseigentümerIn zustimmt, deren Rechte durch die Maßnahme über das in § 14 Nr. 1 WEG bestimmte Maß hinaus beeinträchtigt werden. Gibt es für die anderen WohnungseigentümerInnen keinen über das bei einem geordneten Zusammenleben unvermeidliche Maß hinausgehenden Nachteil, ist nach § 22 Abs. 1 Satz 2 WEG ihre Zustimmung zu der beabsichtigten baulichen Veränderung nicht erforderlich. Nur konkrete und objektive Beeinträchtigungen gelten als ein solcher Nachteil; entscheidend ist, ob sich nach der Verkehrsanschauung ein WohnungseigentümerInnen in der entsprechenden Lage verständlicherweise beeinträchtigt fühlen kann.

Eine Beeinträchtigung der WohnungseigentümerInnen ist nicht bereits deswegen zu verneinen, weil sie ihrerseits in der Eingangshalle eine Kamera angebracht haben, die laufend Videoaufzeichnungen fertigt. Nicht entschieden wurde, ob eine solche Videoüberwachung zulässig ist. Jedenfalls liegt in der einvernehmlichen Videokontrolle eines bestimmten Teils des Wohnhauses nicht die generelle Zustimmung der Wohnungseigentümer zu Eingriffen in ihr Persönlichkeitsrecht durch Ausdehnung der Videoüberwachung auf andere Bereiche. Im vom BGH entschiedenen Fall ging es der Klägerin nicht darum, eine Videokamera zu installieren, die eine dauernde Beobachtung und Kontrolle der anderen Hausbewohner oder sie betreffender Besucher ermöglicht. Vielmehr soll die Kamera nur durch Betätigung der Klingel aktiviert werden können, wobei ein Bild des Eingangsbereichs allein in die Wohnung übertragen werden soll, bei der ein Besucher geklingelt hat. Außerdem soll die Bildübertragung nach einer Minute automatisch unterbrochen werden. Auf diese Weise soll der Klägerin die Möglichkeit verschafft werden, durch eine zeitlich begrenzte Bildübertragung die bei ihr klingelnde Besuchern zu identifizieren und über deren Einlass in das Haus zu entscheiden.

In diesen engen Grenzen bewirkt die Maßnahme keine Beeinträchtigung des Persönlichkeitsrechts der WohnungseigentümerInnen. Es erfolgt weder eine Überwachung des Eingangsbereichs für längere Zeiträume oder mit Regelmäßigkeit noch ist die Videoübertragung darauf angelegt, sämtliche BenutzerInnen des Hauseingangsbereichs abzubilden.

Andere WohnungseigentümerInnen werden nur dann bildlich erfasst, wenn sie sich zeitgleich mit einem bei der Klägerin klingelnden Besucher im Erfassungsbereich der Kamera aufhalten. Durch eine derart zufällige Einbeziehung eines Wohnungseigentümers in die Bildübertragung erleidet sie keinen über das bei einem geordneten Zusammenleben unvermeidliche Maß hinausgehenden Nachteil.

§ 6b BDSG, dessen Wertungen im Rahmen des § 14 Nr. 1 WEG zu berücksichtigten sind, steht der Zulässigkeit der Anbringung der fraglichen Videokamera im Klingeltableau nicht entgegen. Nach § 6b Abs. 1 Nr. 2 BDSG ist die Videoüberwachung öffentlich zugänglicher Räume zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zum öffentlich zugänglichen Raum zählt auch der jedermann zugängliche Eingangsbereich einer privaten Haus- oder Wohnungstür. Die Videoklingelanlage dient dem Zweck, nur solchen Personen Einlass in das Haus zu gewähren, über deren Identität oder Lauterkeit sich die Hausrechtsinhaberin vergewissert hat. Dies kann nicht durch mildere, ebenfalls geeignete Mittel erreicht werden. Auch stehen keine überwiegenden Interessen der die Klingel betätigenden Besucher entgegen, wenn die – zeitlich eng begrenzte – Bildübertragung allein zum Zwecke ihrer Identifizierung und zur Einlasskontrolle durch die angeklingelte Hausbewohnerin erfolgt.

Der Auffassung, ein unzulässiger Eingriff in das Persönlichkeitsrecht der übrigen Wohnungseigentümer sei nur dann zu verneinen, wenn jedwede Manipulation oder Möglichkeit zum anderweitigen Betrieb der Videoanlage von vorneherein ausgeschlossen ist, ist der BGH nicht gefolgt. Allein die fern liegende, mehr oder weniger theoretische Möglichkeit, durch manipulative Eingriffe die Konfiguration der Anlage so zu ändern, dass die Videokamera unabhängig von einem Klingeln aktiviert werden kann, rechtfertigt nicht die Annahme einer über das Maß des § 14 Nr. 1 WEG hinaus gehenden Beeinträchtigung der übrigen WohnungseigentümerInnen. Das bloße Risiko einer Beeinträchtigung ist noch keine Beeinträchtigung. Ein Nachteil liegt erst vor, wenn durch die Videoanlage die Beeinträchtigung einer anderen WohnungseigentümerIn hinreichend wahrscheinlich ist (www.rechtslupe.de 27.05.2011; KN 15.10.2011 WuB I).

BGH

Hostprovider für Persönlichkeitsverletzung verantwortlich

Der Bundesgerichtshof (BGH) stellte mit Urteil vom 25.10.2011 klar, dass sich Opfer von Persönlichkeitsverletzungen im Internet an die Gerichte ihres Heimatlandes wenden können (Az. VI ZR 93/10). Der Betroffener muss dem Provider – hier ging es um Google – darlegen, dass in einem seiner Blogs gegen Recht verstoßen wurde. Dieser Hinweis müsse „so konkret gefasst“ sein, das er „ohne eingehende rechtliche und tatsächliche Überprüfung bejaht werden kann“. Diese Beanstandung muss der Provider dann an den Blog-Verantwortlichen weiterleiten. Äußert sich dieser nicht, muss der Eintrag gemäß der Karlsruher Entscheidung gelöscht werden. Beharrt der Blogger jedoch auf seinen Aussagen, muss der Betroffene sich bemühen, die Rechtsverletzung zu belegen. Kann er das nicht, bleibt der beanstandete Eintrag im Netz, gelingt der Nachweis, muss er gelöscht werden. Für solche Fälle sind demnach deutsche Gerichte zuständig, auch wenn der Provider seinen Sitz im Ausland hat. Google zeigte sich erleichtert darüber, dass das Unternehmen nicht alle Inhalte vorab auf ihre Rechtmäßigkeit prüfen müsse oder Behauptungen schon „auf Zuruf“ löschen müsse. Im konkreten Fall war in einem Mallorca-Blog ein Mann mit voller Namensnennung beschuldigt worden, er habe mit Firmen-Kreditkarte Rechnungen eines Sexclubs bezahlt. Da der Autor nicht bekannt war, verklagte der Betroffene Google als Provider und bekam vom Oberlandesgericht Hamburg Recht. Der BGH hob diese Entscheidung nun auf und verwies sie zur weiteren Prüfung zurück. Ausdrücklich billigten die Karlsruher Richter die Ansicht der Vorinstanzen, dass hier deutsches Recht Anwendung findet (PE BGH Nr. 169 25.10.2011; Müller www.faz.net 25.10.2011).

BGH

Google darf Bilder zeigen, die einmal rechtmäßig im Netz stehen

Der für das Urheberrecht zuständige I. Zivilsenat des Bundesgerichtshofs (BGH) hat am 19.10.2011 erneut entschieden, dass Google nicht wegen Urheberrechtsverletzung in Anspruch genommen werden kann, wenn urheberrechtlich geschützte Werke in Vorschaubildern ihrer Suchmaschine wiedergegeben werden (Az. I ZR 140/10 – Vorschaubilder II). In dem Urteil stellt der BGH klar, dass eine die Rechtswidrigkeit des Eingriffs ins Urheberrecht ausschließende Einwilligung auch dann vorliegt, wenn eine Abbildung eines Werkes von einem Dritten mit Zustimmung des Urhebers ohne Schutzvorkehrungen ins Internet eingestellt worden ist. Der Kläger hatte Dritten das Recht eingeräumt, das Lichtbild im Internet öffentlich zugänglich zu machen. Es sei allgemein bekannt, dass Suchmaschinen, die das Internet in einem automatisierten Verfahren nach Bildern durchsuchen, nicht danach unterscheiden können, ob ein aufgefundenes Bild von einem Berechtigten oder einem Nichtberechtigten ins Internet eingestellt worden ist. Deshalb kann und darf der Betreiber einer Suchmaschine eine solche Einwilligung dahin verstehen, dass sie sich auch auf die Anzeige von solchen Abbildungen in Vorschaubildern erstreckt, die ohne Zustimmung des Urhebers ins Internet eingestellt worden sind. Ein Fotograf habe aber die Möglichkeit, die Veröffentlichung im Internet nur unter der Auflage zu gestatten, dass der Webseitenbetreiber technische Schutzvorkehrungen verwendet, damit ein Foto nicht in Suchmaschinen angezeigt wird. Offen blieb nach dem Urteil, wie Bilder zu beurteilen sind, die komplett illegal im Netz veröffentlicht sind (BGH PE 19.10.2011, juris. bundesgerichtshof.de; www.sat1.de 19.10.2011).

LG Aschaffenburg

Betreiber von Facebook-Fanpages unterliegen Impressumgspflicht

Im Rahmen eines einstweiligen Verfügungsverfahrens stellte das Landgericht (LG) Aschaffenburg mit Beschluss vom 19.08.2011 fest, dass NutzerInnen von „Social Media“ wie Facebook-Accounts nach § 5 Telemediengesetz (TMG) eine eigene Anbieterkennung vorhalten müssen, wenn die Accounts zu Marketingzwecken benutzt werden und nicht nur eine reine private Nutzung vorliegt (Az. 2 HK O 54/11). Im vorliegenden Fall hatte die Antragsgegnerin auf der Facebook-Seite kein eigenes Impressum, sondern nur Angaben zur Anschrift und zur Telefonnummer. Zu den Angaben über den Geschäftsführer der Antragsgegnerin kam man nur über den Punkt „Info“ durch Anklicken zur eigentlichen Website und von da zum Punkt Impressum, dem die verantwortliche juristische Person zu entnehmen war.

Das LG führt dazu aus, dass nach § 5 Abs. 1 Nr. 1 TMG der Dienstanbieter mit Namen, Anschrift und, bei juristischen Personen, der Rechtsform sowie der Vertretungsberechtigte leicht erkennbar sein müssen, was im vorliegenden Fall jedoch nicht der Fall war. Zu den Angaben des Geschäftsführers der Antragsgegnerin kam man nur nach mehreren Schritten auf der Impressums-Seite der Webseite der Antragsgegnerin. Die leichte Erkennbarkeit war damit nicht gegeben. Die Pflichtangaben müssen einfach, ohne langes Suchen und effektiv optisch wahrnehmbar sein. Bezüglich der Bezeichnung des Links sind Bezeichnungen wie z. B. „Nutzerinformationen“ mangels Klarheit abzulehnen. Deshalb liege bereits in der Bezeichnung „Info“ ein Verstoß gegen § 5 Telemediengesetz vor. Es müsse zudem klar sein, auf welche Telemedien sich das Impressum bezieht. Wenn auf ein Impressum verlinkt wird, muss dort auch angegeben werden, dass sich dieses Impressum auch auf die Facebook-Seite bezieht.

Eine Standard-Unternehmensseite bei Facebook sieht keinen Reiter „Impressum“ vor. Vielmehr ist nur der Reiter „Info“ vorhanden, der aber nach Ansicht des LG Aschaffenburg gerade nicht geeignet ist. Bei Twitter hat man gar keine Möglichkeit ein Impressum direkt einzubinden. Es muss daher zumindest sichergestellt werden, dass das verlinkte Impressum sich ausdrücklich auch auf die angebotenen Social Media Seiten bezieht (Schmidt www.it-rechts-praxis.de 27.10.2011).

VG Berlin

Polizei-Namensschilder rechtmäßig

Die umstrittenen Namens- und Nummernschilder für die PolizistInnen Berlins sind zumindest hinsichtlich des Mitbestimmungsrechts nicht zu beanstanden. Das Berliner Verwaltungsgericht (VG) verneinte mit Beschluss vom 16.11.2011, dass die Anweisung nicht mitbestimmungspflichtig ist und wies damit eine Klage des Gesamtpersonalrates der Polizei ab (Az. VG 60 K9.11). Das Gremium hatte moniert, rechtswidrig nicht ausreichend beteiligt worden zu sein. Berlin hatte nach jahrelangen Querelen als erstes Bundesland PolizistInnen verpflichtet, Schilder mit Namen oder einer fünfstelligen Dienstnummer zu tragen (vgl. DANA 1/2011, 19). Der frühere Polizeipräsident Dieter Glietsch hatte eine entsprechende Geschäftsanweisung erlassen. Kompromiss war, dass die BeamtInnen zwischen Nummer und Namen selbst wählen können. Seit Juli 2011 wurde die Kennzeichnung schrittweise eingeführt. Laut Gewerkschaft tragen rund 13.000 Berliner PolizistInnen die Schilder an ihrer Uniform. Sie haben beide Varianten bekommen. Der Bund lehnt dagegen eine individuelle Kennzeichnungspflicht für die BundespolizistInnen ab. Sie würden auch ohne Kennzeichnung in breiten Teilen der Bevölkerung hohes Ansehen genießen.

Der Berliner Kompromiss zum Tragen der Schilder sei ohne den Gesamtpersonalrat von einer Einigungsstelle geschlossen worden, kritisierte dessen Vorsitzender, Karl-Heinz Dropmann. Eine Geschäftsanweisung reiche nicht aus. Laut Verwaltungsrichter Johann Weber ging es bei der Feststellungsklage nicht darum, ob die Kennzeichnung von PolizistInnen sinnvoll oder nicht sei. Da das Tragen der Schilder nicht den Umgang der PolizistInnen untereinander regele, sondern sich auf die Erfüllung ihres Dienstes nach außen – als Service für die BürgerInnen – richte, müsse die Personalvertretung nicht beteiligt werden, begründete er die Ablehnung. Der Gesamtpersonalrat lehnte die Kennzeichnung ebenso ab wie die Gewerkschaft der Polizei (GdP). Sie finden, dass PolizistInnen durch die Identifizierung in der Öffentlichkeit gefährdet seien. Denn BeamtInnen müssten damit rechnen, bedroht zu werden. Auch könnten die Familien der BeamtInnen ausspioniert werden.

Mittlerweile haben sich SPD und CDU in den Koalitionsverhandlungen darauf geeinigt, dass die Nummern künftig in einem festen Rhythmus geändert werden sollen. Wer will, kann aber auch künftig ein Namensschild an der Uniform tragen. Der scheidende Innensenator Ehrhart Körting (SPD) wollte die individuelle Kennzeichnung, damit die Polizei in der Hauptstadt den Menschen noch offener und bürgernaher begegnen könne. Die Berliner GdP kündigte weitere Klagen vor dem VG Berlin von KollegInnen gegen die „Zwangs-Kennzeichnung“ an. Wie Vize-Landeschef Detlef Herrmann sagte, werden derzeit vier Fälle vorbereitet. Diese PolizistInnen haben Widerspruch gegen das Tragen der Schilder eingelegt und ablehnende Antworten bekommen (www.welt.de//regionales/berlin/ 16.11.2011; SZ 17.11.2011, 7).

ArbG Düsseldorf

Heimliches Video nicht verwertbar

Das Arbeitsgericht (ArbG) Düsseldorf entschied am 03.05.2011, dass Aufnahmen aus heimlichen Videoaufzeichnungen eines Arbeitgebers vor Gericht grundsätzlich nicht verwertbar sind (Az. 11 Ca 7326/10). Eine Ausnahme gilt allenfalls, wenn bereits zuvor gegen einen Mitarbeiter der konkrete Verdacht

einer Straftat bestanden hat. Das ArbG gab der Kündigungsschutzklage eines Arbeitnehmers statt. Dessen Arbeitgeber hatte den in einer Brauerei Beschäftigten mittels heimlicher Videoaufzeichnungen überführt, Bier auf eigene Rechnung verkauft zu haben. Das Gericht wertete die daraufhin ausgesprochene Kündigung als rechtswidrig. Der Arbeitgeber habe keinen Beweis für seinen Vorwurf vorgelegt. Das Video sei ein so gravierender Eingriff in das Persönlichkeitsrecht des Mitarbeiters, dass es gerichtlich nicht verwertbar sei. Nur wenn er diesen Mitarbeiter schon konkret im Verdacht gehabt hätte, wäre die Aufzeichnung zulässig gewesen (Kieler Nachrichten 19.11.2011, Anzeigen VI; PM ArbG vom 3.5.2011; ebenso mit gleichem Datum Az. 9 BV 183/10).

Jahrestagung 2011 des FIfF in Kooperation mit der Hochschule München

Dialektik der Informationssicherheit

Unter dem Motto Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit trafen sich vom 11. bis 13. November 2011 an der Hochschule München Expertinnen und Experten aus Wissenschaft, Wirtschaft und Technik mit interessierten Bürgerinnen und Bürgern, um sich von Freitagabend bis Sonntagvormittag mit der Sicherheit von Information und Daten auseinanderzusetzen.

In allen Bereichen der Gesellschaft nimmt der Rechnereinsatz laufend zu; das Internet ist nicht nur für Industrie, Handel und Behörden, sondern auch für den Privatbereich zu einem zentralen Teil der Infrastruktur geworden. Damit ist die Sicherheit der Informationen wichtiger als je zuvor; aber sie ist durch mächtige Interessen bedroht. Auf allen Ebenen entstehen Konflikte.

Der Bayerische Landesbeauftragte für den Datenschutz, Dr. Thomas Petri, beleuchtete in seinem Einführungsvortrag die Vorratsdatenspeicherung aus EU-rechtlicher und verfassungsrechtlicher Perspektive. Er stellte dabei den Weg der Vorratsdatenspeicherung dar: von der mehrmaligen Ablehnung durch den Bundestag, zuletzt im Februar 2005, über die EU-Richtlinie 2006, deren Umsetzung in nationales Recht 2007 und die Ablehnung durch das Bundesverfassungsgericht 2010 bis hin zur heutigen Debatte um Wiedereinführung, Quick-Freeze und Quick-Freeze-Plus. Anschließend diskutierten Constanze Kurz, Sprecherin des Chaos Computer Clubs, Enno Rey von der IT-Sicherheitsfirma ERNW, Michael George, bayerischer Verfassungsschützer im Bereich Wirtschaftsspionage, Thomas Petri und Rainer Gerling, IT-Sicherheits- und Datenschutzbeauftragter der Max-Planck-Gesellschaft. Sie behandelten die Wechselwirkungen der Sicherheitsaspekte Anonymität, Integrität und Vertraulichkeit an konkreten Beispielen aus dem privaten Bereich der Bürger, aus der Wirtschaft und der Arbeit staatlicher Einrichtungen. Wie nicht anders zu erwarten, ergab sich eine lebhafte Diskussion, in der unterschiedliche Wertvorstellungen, unterschiedliche Ziele und unterschiedliche Vorstellungen politischen Handelns aufeinandertrafen.

Am Samstag wurden Einzelaspekte vor allem der Datensicherheit und des Datenschutzes in gut besuchten und informativen Arbeitsgruppen vertieft. Dabei ging es um Datensicherheit bei mobilen Datenträgern, Data-Mining im Internet, Datenschutz in sozialen Netzen, kritische Infrastrukturen und kritische Informationsinfrastrukturen.

Über die Themenbereiche Datenschutz und -sicherheit hinaus gab es Arbeitsgruppen zu EU-Sicherheitspolitik und -forschung, zu Fairen Computern, zu Rüstung und Informatik, und zu den Perspektiven einer europäischen Zusammenarbeit netzpolitischer Gruppen.

Die Sicherheitsbeauftragte eines DAX-Konzerns, Monika Hansmeier, schilderte anschließend in ihrem Vortrag die Fragen der Sicherheit, die in einem Großkonzern zu berücksichtigen sind – von der Security Awareness über organisatorische Vorkehrungen bis hin zu technischen Maßnahmen.

Anschließend zeigte das FIfF in der Münchner Erstaufführung den Film Behind the Screen – das Leben meines Computers. In diesem vom FIfF unterstützten Film wird eindringlich dargestellt, welche Auswirkungen die IT-Industrie im globalen Süden hat: Umweltschäden, Gesundheitsgefährdung bei Menschen und Zerstörung wirtschaftlicher Infrastrukturen sind der Preis, den andere für unseren informationstechnischen Fortschritt bezahlen müssen.

Der FIfF-Studienpreisträger 2010, Phillip Brunst, zeigte am Sonntagmorgen in seinem sehr anschaulichen Vortrag die Konflikte zwischen Anonymität, Integrität und Vertraulichkeit auf der einen und Strafverfolgung auf der anderen Seite. Er ging dabei detailliert auf die Überwachung von Bestands-, Verkehrs- und Inhaltsdaten ein. Sowohl über die technischen Rahmenbedingungen als auch über die einschlägigen gesetzlichen Regelungen gab er einen Überblick, der sich zu einem Rahmen der digitalen Überwachung verdichtete, in den man aktuelle Themen wie Vorratsdatenspeicherung und Online-Durchsuchung einordnen kann.

In einer Begleitausstellung mit Ständen, Videos und Poster-Session ging es um Themen wie Security Awareness, Organisationen, sowie Produkte und Sponsoren der Tagung. Mitarbeiterinnen und Mitarbeiter der Humboldt-Universität Berlin wiesen auf das immer geringer werdende Lehrangebot im Bereich Informatik und Gesellschaft hin, und forderten die Tagungsteilnehmer auf, Lehrangebote und -wünsche für einen virtuellen Studiengang einzureichen.

Den Ausklang bildete wie gewohnt die Mitgliederversammlung des FIfF, bei der in diesem Jahr auch der neue Vorstand gewählt wurde.

In Summe war es wieder eine gelungene Tagung. Die FIfF-Jahrestagung 2012 wird vom 9. bis 11. November 2012 in Fulda stattfinden.

(Dagmar Boedicker, Stefan Hügel)

Buchbesprechung

Spiros Simitis (Herausgeber)
Bundesdatenschutzgesetz – Kommentar
7. neu bearbeitete Auflage 2011, 1886 Seiten, Gebunden mit Schutzumschlag, ISBN 978-3-8329-4183-3, Preis 178,- €



Mit der vorliegenden, neu bearbeiteten Auflage ist die Kommentierung des Standardwerkes zum Bundesdatenschutzgesetz wieder auf den aktuellen Stand gebracht worden. Eine weitere Auflage ist bestimmt zu erwarten, wenn der Bundesgesetzgeber sich zu neuen Regelungen im Bereich des Beschäftigtendatenschutzes durchgerungen hat, beabsichtigt er doch eine Vielzahl von Buchstaben bei § 32 BDSG zu vergeben und damit das Bundesdatenschutzgesetz um eine große Zahl neuer Paragraphen rund um den Umgang mit Beschäftigtendaten zu erweitern. Jedoch ist nicht nur die Kommentierung auf einen aktuellen Stand gebracht, sondern sind aus dem Kreis der Kommentatoren Johann Bizer, Hansjörg Geiger und Stefan Walz leider ausgeschieden. Alle drei verfügen und verfügten über einen hohen Sachverstand im Bereich des Datenschutzrechts und waren dem Themenbereich lange Jahre eng verbunden. Ihr Ausscheiden ist sehr zu bedauern. Geschlossen werden konnte die hierdurch entstandene Lücke durch Achim Seifert, Phillip Scholz und Eugen Ehmann, ebenfalls Personen, denen die Materie und die Fallstricke des Datenschutzrechts nicht unbekannt sind.

Das vorliegende Werk ist als Standardwerk der Kommentarliteratur zum Bundesdatenschutzgesetz nicht nur vom Umfang mit 1886 Seiten sehr „gewichtig“, sondern insbesondere vom Inhalt her. Dabei wird von den Bearbeitern kritisch über den Tellerrand hinausgeschaut und auch auf gesetzgeberische Mängel hingewiesen, wenn es z.B. bei der Kommentierung von Simitis zu § 4 b – Übermittlung personenbezogener Daten ins Ausland, Rdnr. 3 heißt: „Der Gesetzgeber hat vielmehr die Novellierungschance genutzt, um die Übermittlungsschranken der EG-Datenschutzrichtlinie gleich in mehrfacher Hinsicht zu lockern.“. Insoweit zeigen die Kommentatoren sehr genau die Mängel auf, die auch bei einer Revision des Datenschutzrechtes in Deutschland nicht unbeachtet bleiben sollten. Doch eine wirkliche Überarbeitung der nicht sehr normenklaren Materie „Datenschutz“ und des Bundesdatenschutzgesetzes ist derzeit leider nicht zu erwarten, was ein Werk in diesem Umfang mehr als rechtfertigt.

Die Kommentatoren erfassen nicht nur die gesamte Literatur, die es zu den einzelnen Rechts- und Auslegungsfragen bisher gibt, sondern haben fast akribisch auch die Rechtsprechung im Blick, auch wenn sie letztendlich nicht alle Entscheidung erfassen können. So wird zwar zu Recht darauf hingewiesen, dass juristische Personen vom Bundesdatenschutzgesetz – wie bei der EG-Datenschutzrichtlinie – nicht erfasst werden. Jedoch ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts, aber auch der Instanzgerichte (vgl. VG Wiesbaden, Urteil vom 07.12.2007, Az. 6 E 928/07), dass juristische Personen des Privatrechts in der Form der AG, GmbH bzw. GmbH & Co KG sich auf das Recht der informationellen Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und Art. 14 Abs. 1 sowie Art. 19 Abs. 3 GG insoweit berufen können, als ihren Trägern Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der betreffenden individualisierten oder individualisierbaren Daten zusteht. Insoweit wäre es schön, auch hierzu etwas lesen zu können. Dass dem nicht so ist, schmälert jedoch den gesamten Kommentar in seinem Wert nicht.

Gerade wohl auch im Hinblick auf die Geodaten versucht Dammann in § 3, Weitere Begriffsbestimmungen, Rdnrn. 57 ff., eine Abgrenzung von Personen- zu Sachdaten. Dabei weist er zu Recht darauf hin, dass ein Sachdatum je nach Kontext auch ein personenbezogenes Datum sein kann. So kann zum Beispiel auf der Homepage der Hessischen Verwaltung für Bodenmanagement in einem Verfahren „BORIS Hessen“ über die Flur- und Flurstücksbezeichnung eine Adresse ermittelt werden und dies, obwohl das Verfahren nur über die Bodenrichtwerte informieren soll. Würde die Flur- und insbesondere die Flurstücksnummer entfallen und ein Grundstück in einer Menge von Grundstücken untergehen, so handelte es sich mit Sicherheit um ein Sachdatum; so aber sind die gelieferten Informationen auf Grund des hohen Detaillierungsgrades ein personenbezogenes Datum. Das heißt: Bei einer Maßstabsveränderung in einen größeren Maßstab wäre eine Zuordnung nicht mehr möglich. Damit besteht jedoch für den Anwender das Problem, dass er sich im Einzelfall doch Gedanken machen und selbst entscheiden muss, ob ein Sachdatum oder ein personenbeziehbares und damit personenbezogenes Datum vorliegt. Ein Ergebnis, welches im Hinblick auf die Komplexität des Lebens nicht befriedigend ist, aber immer wichtiger wird. Immerhin bietet, wie das Beispiel zeigt, das Werk auch insoweit Hinweise und Lebenshilfe in einem.

Natürlich wird an den passenden Stellen auch auf das jeweilige Datenschutzrecht der Länder hingewiesen, steht doch das Bundesdatenschutzgesetz nicht alleine, sondern gibt es allein im Rahmen des Föderalismus noch weitere 16 Landesdatenschutzgesetze; von der Vielzahl bereichsspezifischer Normen gerade auch im Bereich der Sozialgesetzbücher ganz zu schweigen.

Damit gehört der vorliegende Kommentar zu dem notwendigen Handwerkszeug nicht nur von Daten-

schutzbeauftragten, sondern aller Juristen, die sich mit datenschutzrechtlichen Fragen befassen, zur Pflichtlektüre in den Ministerien und bei den Abgeordneten. Gerade letztere erhalten mit dem vorliegenden Werk auch einen guten Überblick, wie man das Bundesdatenschutzgesetz normenklarer gestalten kann als es der Gesetzgeber bisher geleistet hat. Forderte doch schon das Bundesverfassungsgerichte „normenklare Regeln".

Damit kann man getrost sagen: Der neue Simitis ist da, packen wir ihn an.

Bernhard C. Witt,
Datenschutz kompakt und verständlich – Eine praxisorientierte Einführung mit Online-Service,
2010, 2., aktualis. u. erg. Aufl., XII, 246 Seiten, 61 Schwarz-Weiß-Abbildungen, Maße: 17,4 x 24,5 cm, Kartoniert (TB), Deutsch Vieweg+Teubner
ISBN-10: 3834812250; ISBN-13: 9783834812254, 24,95 €



Der Autor des vorliegenden Werkes, Bernhard C. Witt, ist Diplom-Informatiker und Lehrbeauftragter für Datenschutz und IT-Sicherheit an der Universität in Ulm. In dem Vorwort heißt es: „Meine Lehrveranstaltung wie auch dieses Buch sollen dazu befähigen, tägliche Anforderungen der Berufspraxis im Bereich des Datenschutzes meistern zu können."

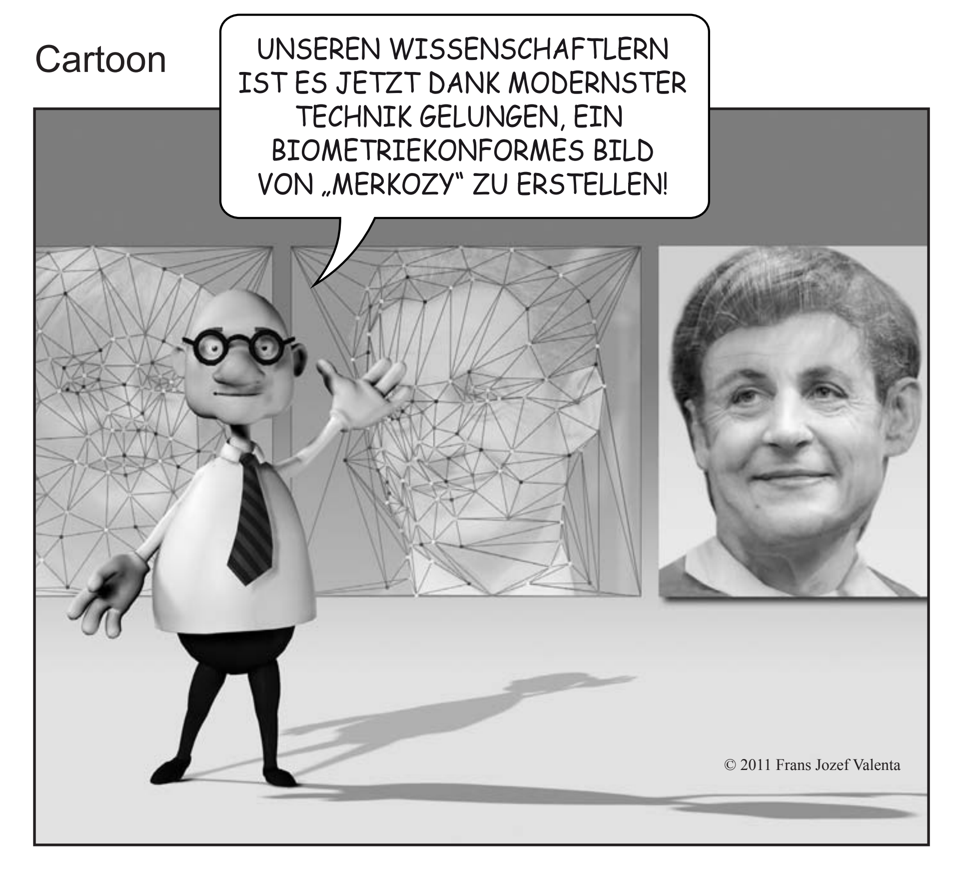
Ob das Werk zum „meistern" ausreichend ist, mag durchaus zu bezweifeln sein. Jedoch liefert das Werk eine Grundlage, um ggf. gestützt auf weitere Informationen das schwierige Themengebiet Datenschutz mit all seinen Facetten oder vielleicht besser Untiefen meistern zu können.

Für einen Juristen dürfte die Art, wie der Autor sich dem Thema nähert, etwas fremd sein. Sie entspricht vielleicht mehr dem Ansatz eines Informatikers und dürfte auch Beleg dafür sein, wie sich der Autor selbst das Thema erschlossen hat. Dabei wird nicht nur das Bundesdatenschutzgesetz vorgestellt, sondern der Sozialdatenschutz ebenso in den Fokus genommen wie der Datenschutz im Internet, der Mediendatenschutz oder gar datenschutzfreundliche Techniken.

Damit bietet das Werk einen guten Einblick in die komplexe Materie. Soweit die Überschrift des Werkes von einem „verständlichen" Datenschutz spricht, sind es insbesondere die Schaubilder, die dem Leser die verbalen Ausführungen verständlich machen. Jedoch kann das Werk nicht zur alleinigen Grundlage datenschutzrechtlicher Tätigkeit gemacht werden, zumal sich trotz guter Ansätze auch Fehler bzw. mögliche Missverständnisse eingeschlichen haben. So zeigt die Abbildung Nr. 11 (Zusammenspiel von Grundrechten bei der Mail-Kommunikation) die Geltung des Fernmeldegeheimnisses so, als ob dieses nur von Provider zu Provider gilt. Eine Auffassung, die nach einer der ersten Entscheidungen des Bundesverfassungsgerichts vertreten wurde, da es dort um den Mailzugriff beim Provider ging. Spätestens mit dem Beschluss vom 16.06.2009 steht jedoch fest, dass der Schutz des Fernmeldegeheimnisses grundsätzlich erst in dem Moment endet, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist. Befindet sich die E-Mail auf dem PC des Empfängers, so hat dieser es dann in der Hand, die E-Mail auf dem Rechner gespeichert zu lassen oder nicht. In diesem Fall würde dann erst das informationelle Selbstbestimmungsrecht Anwendung finden.

Eine solche leichte Unschärfe schmälert jedoch den Wert des Werkes nicht. Den versprochenen Online-Service zu dem Buch unter www.informatik.uni.ulm.de/datenschutz/lehrbuch/datenschutz konnte der Rezensent leider nicht finden. Trotzdem sei das Werk all denen empfohlen, die sich des Themas Datenschutz im Allgemeinen und Besonderen mehr von der praktischen Seite nähern wollen. Dazu ist das Werk als Basisgrundlage wirklich kompakt und verständlich.

Cartoon



Gemeinsame Presseerklärung des Berufsverbandes der Datenschutzbeauftragten Deutschlands e.V., der Deutschen Vereinigung für Datenschutz e.V. und der Gesellschaft für Datenschutz und Datensicherheit e.V.

Deutsche Datenschutzorganisationen fordern europäische Mindeststandards beim Beschäftigtendatenschutz.

Bonn/Berlin, 20.10.2011

Im Europäischen Parlament in Brüssel erörterten gestern Datenschutzverbände mit Europäischen Abgeordneten die Möglichkeiten der Einbindung des Beschäftigtendatenschutzes in europäische Regelungen. Die Veranstaltung fand auf Initiative der Deutschen Vereinigung für Datenschutz e.V. (DVD) und auf Einladung der Europaabgeordneten Cornelia Ernst statt.

Der Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD), die DVD und die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) diskutierten dabei neben der Einladerin mit den Abgeordneten Birgit Sippel und Jan-Phillip Albrecht, Armin Duttine als Vertreter des Europäischen Wirtschafts- und Sozialausschusses und dem für Datenschutz zuständigen Direktor der Generaldirektion Justiz der Europäischen Kommission, Herrn Paul Nemitz.

Anlässlich dieses Expertengesprächs betonten alle drei großen deutschen Datenschutzvereinigungen gemeinsame Positionen. GDD, BvD und DVD forderten übereinstimmend, dass grundlegende Mindeststandards zum Schutz von Beschäftigten auf europäischer Ebene verbindlich verankert werden müssten. Sie setzten sich außerdem dafür ein, dass nationale Verbesserungen darüber hinaus möglich sein sollen, ohne jedoch hinter die Mindeststandards zurückzufallen.

Beispielhaft wurden in diesem Sinne Mindeststandards diskutiert, die nach übereinstimmender Meinung in vielen weiteren Bereichen entwickelt und etabliert werden müssen:

- Die Möglichkeit, eine Datenverarbeitung im Arbeitsverhältnis auf eine Einwilligung von Beschäftigten zu stützen, darf allenfalls in streng begrenzten Ausnahmefällen zugelassen werden.
- Die Durchführung medizinischer Untersuchungen von Beschäftigten muss sich streng an dem für den jeweiligen Arbeitsplatz erforderlichen Maß orientieren. Das Patientengeheimnis muss jederzeit gewahrt sein.
- Die behördlichen Kontrollmöglichkeiten müssen dem Gefährdungspotenzial entsprechen: je stärker grenzübergreifende Datentransfers erleichtert werden, desto größer muss die Kontrolldichte sein, damit systematischer Missbrauch vereinfachter europäischer Regelungen unterbunden werden kann.
- Die Europäisierung des Modells betrieblicher Datenschutzbeauftragter, der als fachkundiger, unabhängiger Experte das Unternehmen zu datenschutzgerechter Organisation und Umsetzung führen soll, wurde von allen Anwesenden begrüßt.



Am 19.10.2011 führt die DVD im Europäischen Parlament in Brüssel eine Veranstaltung zur Integration des Arbeitnehmerdatenschutzes in zukünftige europäische Regelungen durch.
Es geht darum, Europaabgeordneten darzulegen, warum Beschäftigtendatenschutz unbedingt Teil jeder zukünftigen europäischen Regelung sein sollte – sei es nun eine Richtlinie oder eine Vollregelung.

Da die Deutsche Vereinigung fuer Datenschutz e.V. – DVD selbst keine Veranstaltungen im Parlament durchführen kann, sind wir sehr dankbar, dass Cornelia Ernst (MEP, Linksfraktion) formal die Gastgeberrolle übernimmt.

Als Berichterstatter für Ihre Fraktionen haben neben Cornelia Ernst als Gastgeberin bereits Alexander Alvaro, Jan Phillipp Albrecht und Armin Duttine als Vertreter des Berichterstatters Peter Morgan für das EESC seine Teilnahme zugesagt.

Wir werden mit einer einstündigen Runde beginnen, die den Berichterstattern die Gelegenheit geben soll, den Teilnehmern ihre Position darzulegen.

Anschließend werden wir das Podium erweitern und „ins Detail gehen" – und zwar mit

- Peter Gola, Vorsitzender der GDD
- Thomas Spaeing, Vorsitzender des BVD
- Karin Schuler, Vorsitzende der DVD

Die grundlegende Position der DVD findet sich in der Stellungnahme zum Vorhaben der Kommission, die Richtlinie 95/46/EC zu novellieren:

www.datenschutzverein.de/Themen/Stellungnahme EURiLi DVD.pdf

Hierzu Prof. Peter Gola, Vorsitzender der GDD: „ Dies ist zwar eine Lösung, mit der wir besonders in Deutschland sehr vertraut sind, aber gerade wegen der positiven Erfahrungen können wir sie uneingeschränkt für den gesamten europäischen Raum empfehlen." Wichtig sei, die in der EU-Datenschutzrichtlinie verankerte Unabhängigkeit der Datenschutzkontrollinstanzen für den Datenschutzbeauftragten EU-rechtlich zu konkretisieren und die Außerachtlassung von Vorabkontrollen zu sanktionieren.

Es wurde allgemein abgelehnt, Datenschutz hinter die Wirtschaftsförderung zurückzustellen. Karin Schuler, Vorsitzende der DVD merkte hierzu an: „Solange ein Datenschutzverstoß gleichsam ‚aus der Portokasse' bezahlt werden kann, darf der europäische Gesetzgeber sich nicht auf die Einsicht der Unternehmen alleine verlassen. Thomas Spaeing, Vorsitzender des BvD, ergänzte: „Spätestens wenn Datenschutz als wirtschaftsfeindlich bezeichnet wird, ist es Zeit für den Gesetzgeber, Flagge zu zeigen und klarzustellen, dass es wirtschaftlichen Erfolg ohne Schutz der Beschäftigten nicht geben kann."

Die anwesenden Experten sowie die Vertreter des Parlaments und der Kommission waren sich einig, dass die Diskussion fortgesetzt werden soll. Herr Nemitz betonte außerdem das fortbestehende Interesse der Kommission, die grundlegende Neugestaltung des europäischen Datenschutzrechtes mit den Verbänden der Zivilgesellschaft zu diskutieren und Anregungen aufzunehmen.



Birgit Sippel, MdEP · Karin Schuler, DVD · Cornelia Ernst, MdEP





Thomas Spaeing, BvD





Armin Duttine, EU Wirtschafts-/Sozialausschuss · Jan-Phillip Albrecht, MdEP



Prof. Peter Gola, GDD · Paul Nemitz, EU-Kommission, DG Justiz

Die EU spinnt!

Unschuldsvermutung

Datenschutz

Verhältnismäßigkeit

SMS

Investigativer Journalismus

Unbefangenes Leben

Seelsorger

Privatsphäre

Sechs Jahre Vorratsdatenspeicherung.

Gestaltung: Frans Valenta, www.artbyte.de